Conseil de
l'Union européenne

Bruxelles, le 22 novembre 2024
(OR. en)

15941/24

COSI 214
ENFOPOL 463
IXIM 234
CATS 109
COPEN 500
CYBER 342
DATAPROTECT 332

NOTE

Origine:	la présidence
Destinataire:	délégations
Nº doc. préc.:	11281/24
Objet:	Rapport final du groupe de haut niveau sur l'accès aux données en vue d'une répression efficace

Au nom des coprésidents du groupe de haut niveau (GHN) sur l'accès aux données en vue d'une répression efficace, la présidence présente aux délégations le rapport final du GHN figurant en annexe.

ANNEXE

Rapport final du groupe de haut niveau sur l'accès aux données en vue d'une répression efficace

15 novembre 2024

Les points de vue exposés reflètent exclusivement l'opinion des experts du groupe de haut niveau et ne sauraient être considérés comme représentatifs de prises de position formelles de la Commission européenne ou du Conseil.

Les recommandations formulées par le groupe de haut niveau sur l'accès aux données en vue d'une répression efficace doivent être mises en œuvre dans le plein respect des compétences des États membres. Elles ne s'appliquent qu'aux activités répressives et aux outils commerciaux utilisés à des fins judiciaires et sont sans préjudice de la responsabilité exclusive des États membres en matière de sécurité nationale. Les outils souverains et les outils utilisés et/ou développés exclusivement à des fins de sécurité nationale sont donc exclus du champ d'application des présentes recommandations.

Contents

Synthèse

L'Union européenne constitue un espace de liberté, de sécurité et de justice dans lequel les droits fondamentaux et les différents systèmes et traditions juridiques des États membres sont respectés. Elle œuvre pour assurer un niveau élevé de sécurité[1] par des mesures de prévention de la criminalité et pour faciliter la coordination et la coopération entre les services répressifs, les autorités judiciaires et les autres autorités compétentes.

Les évolutions technologiques et la numérisation de nos sociétés ont entraîné à la fois des changements importants dans la vie quotidienne des citoyens et de nouveaux défis dans la mission incombant aux services répressifs et les autorités judiciaires de garantir un niveau élevé de sécurité, tant au niveau national qu'au niveau de l'UE. Aujourd'hui, presque toutes les enquêtes pénales comportent une composante numérique. Cette question a été abordée en avril 2023 dans le document de cadrage destiné au groupe d'experts de haut niveau sur l'accès aux données en vue d'une répression efficace:

Les technologies et les outils [...] font également l'objet d'abus à des fins criminelles. Du fait de cette évolution, il est de plus en plus difficile de maintenir des services répressifs efficaces dans l'ensemble de l'UE afin de préserver la sécurité publique et de prévenir et détecter les infractions pénales, d'enquêter sur celles- ci et de poursuivre leurs auteurs, et de répondre aux attentes légitimes des victimes en matière de justice et d'indemnisation. Sans réaction suffisante, le véritable risque est que cette tendance actuelle ne permette aux criminels de cesser toute communication sur les canaux publics […]. Il s'agit d'une menace grave pour la sécurité des personnes et de la société, qui peut, à terme, entraver l'obligation positive qu'ont les États de continuer de veiller à l'état de droit et à une société démocratique[2].

[1] Aux fins du présent document, on entend par "sécurité" la lutte contre la criminalité ou la prévention de menaces pour la sécurité publique.

[2] 8281/23 du 13 avril 2023.

Le droit au respect de la vie privée et familiale, du domicile et des communications, ainsi que le droit à la protection des données à caractère personnel, sont garantis par la charte des droits fondamentaux de l'Union européenne. La confidentialité des communications, que ce soit par écrit ou par téléphone, a été une réalisation majeure des sociétés démocratiques, garantissant que ni l'État ni les acteurs privés ne peuvent interférer dans la liberté d'expression des populations et permettant l'établissement d'une société civile vigoureuse. La jouissance de ces droits peut faire l'objet de limitations prévues par la loi, notamment en ce qui concerne les mesures destinées à sauvegarder la sécurité nationale, la défense ou la sécurité publique et pour la prévention et la détection des infractions pénales ou des utilisations non autorisées de systèmes de communications électroniques, et les enquêtes et poursuites en la matière, pour autant que ces mesures soient nécessaires, appropriées et proportionnées au sein d'une société démocratique. Par conséquent, les autorités répressives et judiciaires peuvent ouvrir et lire des communications écrites, intercepter des appels téléphoniques et écouter des conversations, si elles le jugent nécessaire, proportionné et justifié, si ces mesures sont conformes aux dispositions légales applicables et si elles sont appliquées dans le respect des droits fondamentaux. Cette possibilité devrait être ouverte à toutes les autorités compétentes, quelles que soient les évolutions technologiques. La prolifération de nouvelles formes de communication interpersonnelle qui s'est produite ces dernières années signifie que toute la société doit s'adapter aux nouvelles réalités. Nous devons nous assurer que les communications entre les citoyens restent protégées et, dans le même temps, que les services répressifs et les autorités judiciaires continuent de pouvoir remplir leur mission de protection des citoyens en prévenant la grande criminalité organisée et le terrorisme et en luttant contre ces phénomènes. La nécessité d'une adaptation est urgente et les experts invitent les décideurs politiques à agir rapidement, les services répressifs accusant déjà un retard par rapport au rythme des évolutions technologiques, ce qui a une incidence directe sur leur capacité à faire respecter les droits des citoyens.

Lors de la réunion informelle des ministres de la justice et des affaires intérieures du 26 janvier 2023, les ministres de l'intérieur ont examiné les défis que les avancées technologiques posent aux services répressifs à l'ère numérique. Ils se sont également déclarés préoccupés par le fait que les règles applicables et leur interprétation par la jurisprudence, combinées aux obstacles pratiques et opérationnels, compliquent de plus en plus la tâche des services répressifs, en particulier en ce qui concerne la conservation et l'accès aux données nécessaires aux enquêtes et aux poursuites en matière de criminalité[3].

[3] Voir le document 7184/1/23 du 23 mars 2023 pour une compilation des observations des États membres.

À l'issue de ce débat, le Conseil a approuvé la création d'un groupe chargé d'élaborer une vision stratégique prospective sur l'accès effectif et licite aux données, aux preuves électroniques et aux informations à l'ère numérique pour les autorités judiciaires et répressives: le **groupe de haut niveau (GHN) sur l'accès aux données en vue d'une répression efficace[4].**

L'objectif du GHN était de trouver des solutions au défi inhérent à l'autorisation d'un accès légal aux données afin de maintenir un niveau élevé de sécurité pour toutes les personnes vivant dans l'UE, tout en garantissant le respect des droits fondamentaux, y compris les droits au respect de la vie privée et à la protection des données, ainsi qu'un niveau élevé de cybersécurité, grâce à des solutions efficaces et à l'épreuve du temps.

Les **42 recommandations**[5], principal résultat des travaux du GHN, arrivent à un moment où les appels en faveur de la responsabilité en ligne augmentent. Ces recommandations répondent aux défis actuels et à ceux auxquels il faut s'attendre compte tenu des évolutions technologiques, l'objectif étant de permettre une approche globale de l'UE pour garantir l'efficacité des enquêtes et poursuites pénales. Les recommandations sont regroupées en trois blocs: **renforcement des capacités; coopération avec l'industrie et normalisation; et mesures législatives.** Elles soulignent les difficultés rencontrées par les services répressifs pour accéder aux données dans un format lisible pour les enquêtes pénales en raison de l'absence d'obligations harmonisées en matière de conservation des données et d'exigences strictes de la jurisprudence de l'UE, de l'utilisation croissante du chiffrement de bout en bout et du manque de coopération de certains services de télécommunications non traditionnels. Tout en se félicitant des règles relatives aux preuves électroniques, les recommandations soulignent les limites qu'elles présentent pour relever les défis posés par le chiffrement et appellent à une coopération plus étroite entre les autorités répressives et judiciaires et les prestataires de services afin de favoriser un dialogue permanent et une compréhension mutuelle des besoins opérationnels, techniques et commerciaux et de surmonter les difficultés d'accès aux données chiffrées. Selon les experts, une coopération renforcée entre les services répressifs et les prestataires de services améliorera la situation dans une certaine mesure, mais une solution à l'épreuve du temps exige également que les obligations de coopération incombant aux fournisseurs de services aient force de loi, sans affaiblir le chiffrement de manière généralisée ou systématique pour les utilisateurs d'un service.

---

4 High-Level Group (HLG) on access to data for effective law enforcement - Commission européenne (europa.eu).

5 Recommandations du groupe de haut niveau.

Le 13 juin 2024, **le Conseil a procédé à un échange de vues** sur les recommandations du GHN, a largement salué le travail accompli par les experts du GHN et a souligné la nécessité de faire rapidement avancer les travaux sur l'accès aux données en vue d'une répression efficace[6]. Les ministres de l'intérieur ont retenu les priorités suivantes: 1) établir un cadre juridique harmonisé au niveau de l'UE pour la conservation des données à des fins répressives; 2) établir des règles pour un accès effectif aux données relatives aux communications électroniques interpersonnelles; et 3) mettre en place des solutions solides du point de vue juridique et technique pour accéder à des communications électroniques chiffrées dans des cas individuels et sous réserve d'une ordonnance judiciaire aux fins de la prévention de la grande criminalité organisée et du terrorisme, ainsi que des enquêtes et des poursuites en la matière.

En outre, les ministres ont plaidé en faveur d'un renforcement de l'impact de l'UE sur la normalisation des protocoles et des technologies et d'une approche coordonnée en matière de certification des outils et procédures de criminalistique numérique. Enfin, ils ont insisté sur la nécessité d'élaborer une feuille de route pour la mise en œuvre des recommandations, comprenant un calendrier concis et une évaluation de la faisabilité et des ressources financières adéquates. Il a également été jugée important d'assurer la coordination dans la mise en œuvre des différentes recommandations.

L'objectif du présent rapport final est de décrire en détail les défis recensés par les experts et de définir des options pour poursuivre les travaux et **mettre en œuvre les recommandations**. Il décrit plusieurs questions clés recensées par les experts, qui ont guidé trois axes de travail conformément au mandat du GHN.

Premièrement, l'accès aux données est essentiel à la **criminalistique numérique**, pour permettre aux services répressifs de recueillir et d'analyser des preuves provenant d'appareils électroniques. Ces données fournissent des informations fiables sur les activités criminelles et permettent d'identifier les responsables d'actes criminels. Les progrès rapides et l'utilisation généralisée de certaines technologies, telles que le chiffrement, exigent des services répressifs qu'ils renforcent leurs ressources, leurs compétences et leurs solutions techniques en ce qui concerne l'accès aux données chiffrées. À cet égard, et en ce qui concerne l'utilisation de solutions commerciales, une coopération transfrontière efficace peut apporter un soutien grâce au partage d'expertise, à la mise au point d'outils et de procédures normalisés et à la mise en commun de ressources. Toutefois, les experts ont été d'accord sur l'idée que le renforcement des aptitudes organisationnelles ne permettra pas, à lui seul, d'améliorer les capacités des services répressifs. Certains experts ont estimé que permettre l'accès aux données dans un format lisible dans certaines circonstances clairement réglementées constituait une solution à long terme plus durable.

---

[6] Doc. 11281/24 du 21 juin 2024.

Deuxièmement, une législation harmonisée et cohérente en matière de **conservation des données**, pleinement conforme aux droits fondamentaux, est nécessaire pour permettre aux services répressifs de mener les enquêtes et les poursuites avec efficacité en matière criminelle. Du fait de l'évolution rapide des technologies, il est de plus en plus précieux pour les services répressifs d'accéder en temps utile aux données pertinentes stockées par les fournisseurs. En particulier, l'accès aux métadonnées de communication stockées par les fournisseurs de services est essentiel pour identifier les suspects et comprendre leurs activités, et son importance dans l'avancement des enquêtes a été démontrée.

Troisièmement, l'**interception légale** est essentielle pour mener des enquêtes et engager des poursuites efficaces contre la criminalité organisée et les groupes terroristes. Elle permet aux autorités, sur décision judiciaire et dans le plein respect des droits fondamentaux, de demander aux fournisseurs de services de transmettre le contenu d'une communication; or, ce contenu offre des informations précieuses sur les activités criminelles. Compte tenu de l'évolution faisant passer des fournisseurs de communications traditionnels aux services "par contournement" (over-the-top ou OTT), tels que définis dans le code des communications électroniques européen (CCEE)[7], et du fait que les criminels se tournent de plus en plus vers des plateformes chiffrées de bout en bout[8], l'accès légal aux communications en temps réel nécessite d'évaluer la nécessité de règles claires de coopération entre les services répressifs et les entreprises technologiques, ainsi qu'une coopération renforcée au niveau de l'UE afin de faciliter les demandes transfrontières.

Les recommandations et le contenu du présent rapport final reflètent **les attentes et les demandes des seuls experts du GHN**.

Par la présentation de ce rapport, **le GHN a achevé ses travaux** et invite la Commission, les États membres, le Parlement européen et toutes les parties prenantes concernées à s'inspirer des recommandations et du rapport lorsqu'ils élaborent des mesures visant à réglementer la question de l'accès aux données en vue d'une répression efficace. Ces mesures devraient s'accompagner d'un discours fort démontrant qu'il est urgent de prendre des mesures significatives pour garantir de manière effective un accès légal aux données. Les experts encouragent l'ensemble des institutions et organes de l'UE à franchir sans tarder une étape supplémentaire, par la mise en œuvre d'initiatives concrètes dans le cadre d'une feuille de route spécifique.

---

7 Directive (UE) 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen.

8 Rapport d'Europol sur l'évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA) de 2024.

Lawful access: the key challenges

Our ability to fight crime and keep the EU secure has improved in many areas in recent years. Law enforcement and judicial cooperation have become more effective, new legislation and tools to fight serious and organised crime have been put in place, and joint efforts to fight migrant smuggling, trafficking in human beings, firearms and drugs, corruption and other serious crimes have been strengthened.

However, every day, law enforcement authorities face new challenges in keeping our citizens safe, especially those brought about by the digitalisation of our society.

Digital technologies are changing our lives – from the way we communicate to how we live and work – and the societal aspects of this shift are profound. Digitalisation has the potential to provide solutions for many of the challenges Europe and Europeans are facing, and it offers a great many opportunities – opportunities to create jobs, advance education, boost competitiveness and innovation, fight climate change, facilitate the green transition and more.

However, digitalisation also provides the conditions for criminals to exploit technological advances in order to commit crimes both online and offline. Encrypted devices and apps, new communications operators, Virtual Private Networks (VPNs), etc. are designed to protect the privacy of legitimate users. But they also provide criminals with effective means to hide their identities, market their criminal products and services, channel payments and conceal their activities and communications, effectively avoiding detection, investigation and prosecution. While there are tools and services purposely built and primarily used to carry out illegal activities, there is evidence that criminals are increasingly taking advantage of privacy-protecting measures made available by legitimate electronic communications services (ECS). ***Law enforcement agencies often lag behind criminals in this regard, as they lack the appropriate staff, tools and means to address this challenge effectively***. As a result of these developments, access to data for law enforcement purposes has emerged in recent years as a key challenge for criminal investigations and prosecutions. Nevertheless, there have been remarkable successes: for instance, LEAs have managed to dismantle encrypted communication networks of a criminal nature such as EncroChat and SkyECC, and they continue to pursue operations like ‘Desert Light’, during which a ‘super cartel’ of cocaine traffickers was taken down in November 2022. Europol’s Decryption Platform has supported several high-level investigations over the last few years, contributing to successful law enforcement actions against terrorism and serious and organised crime.

However, hidden behind those success stories are many delayed and unsuccessful investigations, as practitioners have reported persistent challenges in meeting operational needs in a timely manner.

By enabling authorities to monitor and intercept criminal communications in a targeted manner and to disrupt criminals' actions, lawful access makes using technology for criminal purposes more difficult. By contrast, without a sound legal framework and adequate resources, LEAs will continue to struggle with insurmountable difficulties, and there is a risk that critical evidence remains out of reach, for a variety of reasons.

- **Data is not always available**, especially when deleted, due to inconsistent and inadequate data retention rules for law enforcement purposes. This gap severely hampers investigations into serious and organised crime. In fact, in the survey conducted in the framework of the SIRIUS project in 2023[9], nearly half of the investigators consulted cited the absence of a harmonised data retention regime as their primary obstacle. Without harmonised rules, there is a risk that crucial data remains out of reach, undermining efforts to combat crime effectively.

- **Data cannot be retrieved**, particularly when extraction from a device fails. The absence of necessary skills, appropriate tools and sufficient cooperation with and by device manufacturers makes digital forensics arduous, expensive and time-consuming, if not entirely impracticable. This significant shortcoming hinders effective investigations. Without advanced forensic capabilities and skills and improved collaboration with industry and between national authorities, crucial digital evidence remains inaccessible, severely impacting law enforcement efforts.

- **Data cannot always be read** due to encryption. Many services now use end-to-end encryption to protect confidentiality of communication, privacy and cybersecurity, but this can make it extremely difficult for law enforcement to access communication data. This means that even if data is intercepted legally, it is often impossible to decode it. Without the ability to read this data, important evidence remains hidden, making it much harder to investigate crimes.

[9] SIRIUS Cross-Border Access to Electronic Evidence (SIRIUS project), https://www.europol.europa.eu/operations-services-innovation/sirius-project.

- **Data cannot always be analysed**, e.g. technology and/or human resources are not always available to screen large quantities of data or to filter and analyse seized data in an effective way that is compatible with the EU's fundamental values and the EU's and Member States' legal frameworks.

- **Data cannot be obtained** due to conflicts of laws between jurisdictions. Data often crosses international borders, creating complex jurisdictional challenges. Different countries have varying laws and regulations regarding data access, making it difficult to obtain data stored abroad. The new EU e-evidence Regulation and Directive are important steps towards making this easier, but a lot of work still needs doing to fully implement these measures – and without full implementation, accessing crucial data from other countries remains a significant challenge for law enforcement.

These are some of the daily challenges that LEAs face today.

Criminals constantly adapt their behaviours to elude detection. Available statistics[10] indicate that criminals are increasingly moving to legitimate end-to-end encrypted platforms. However, once effective countermeasures are found, it is likely that they will move again to different communication channels. For this reason, it is paramount that law enforcement, assisted by experts from all relevant communities, are able to monitor technological developments and anticipate changes in criminal behaviour, such as those linked to 6G, Internet of Things (IoT) and satellite communications. Moreover, the capacities that have enabled successful operations against dedicated criminal communication services (e.g. EncroChat, Ghost ECC) need to be maintained and adapted to face future similar challenges.

[10] Europol IOCTA 2024.

Law enforcement increasingly needs to be able to lawfully access digital information. As criminals rely more and more on online services, requests for data from online service providers are increasing in number; indeed, such requests tripled between 2017 and 2022[11]. Communications data (both metadata and content data) is crucial for many criminal investigations. Access to digital evidence is considered to play a key role in 85 % of investigations[12]. The new set of rules on cross-border access to electronic evidence will increase competent authorities' ability to access that data. However, these rules can only work when the data is available in a readable format. Likewise, access to data stored in seized devices and lawful interception of communications remain remarkably challenging, both legally and practically. When it comes to effectively intercepting data in transit in cross-border cases, Member States can request judicial cooperation via the Mutual Legal Assistance Convention[13] and the European Investigation Order[14]; however, these instruments have mostly been designed with the exchange of physical evidence in mind, and their effectiveness might be limited in the context of technological developments.

Lawful access must be subject to strict conditions, enshrined in national, EU and international law, and transparent and accountable processes must be in place to regulate such access, including by preventing any unlawful disclosure of trade secrets and, in the event of lawful disclosure, ensuring that appropriate measures are taken to maintain their confidentiality.

Lawful access must fully respect the principles of necessity and proportionality and be subject to the approval of a court or an independent authority when necessary. Access to data must be balanced with robust privacy protections and cybersecurity measures (e.g. encryption, firewalls and antivirus and anti-malware software). Ensuring that data access is limited to what is necessary for the purpose of an investigation helps safeguard the privacy of individual users.

---

11 SIRIUS project.

12 Commission Impact Assessment on the Proposals for an e-Evidence Regulation and an e-Evidence Directive (17 April 2018).

13 MLA - Council of Europe standards - PC-OC (coe.int).

14 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0041.

While lawful access to data for law enforcement purposes is at the core of providing our citizens with the highest possible level of security, this must not be at the expense of fundamental rights or the cybersecurity of systems and products. There must be no trade-off between the protection of people's personal integrity and security, on the one hand, and their rights, on the other; it is necessary to find a balance that ensures that one does not encroach on the other. The EU and Member States alike have a duty to ensure that citizens can enjoy a high level of protection of their fundamental rights and that they feel safe in their daily life. Technological developments must not create safe havens for criminals: where there is reasonable suspicion that a crime has been or is about to be committed, law enforcement must have access to tools that enable them to access the relevant data.

The European Convention on Human Rights, national constitutions and the EU Charter of Fundamental Rights all recognise that everyone has the right to a private life, and that this includes a person's communications. The EU Charter of Fundamental Rights also lays down the right to data protection. The rights to privacy and to the protection of personal data are not absolute rights but must be considered in relation to their function in society[15]. Public authorities may not interfere with the exercise of these rights ***except where such interference is in accordance with the law, respects the essence of the rights and is necessary and proportionate in a democratic society.*** Subject to those conditions, the rights to privacy and to the protection of personal data can be limited, including in the interest of national and public security and for the prevention, investigation, detection and prosecution of crime.

Strong accountability is crucial. In our democratic societies, it is the responsibility of lawmakers to establish the conditions for such accountability, ensuring a high level of privacy and security. ***Privacy and security are not mutually exclusive***.

Solutions to ensure lawful access in justified cases need to be devised in cooperation with all relevant stakeholders, including industry, in order to promote innovation and strong cybersecurity. ***These solutions must be designed taking into due account all relevant needs and requirements and cannot be left to the sole discretion of technology companies***.

---

[15] Judgment of 30 April 2024, *La Quadrature du Net and Others () and lutte contre la contrefaçon)*, Case C-470/21 EU:C:2024:370, para. 70.

Technical assessments must be carried out before further steps can be taken, in order to address the concerns of some cybersecurity experts regarding the complexity of ensuring lawful access while maintaining strong cybersecurity. ***Cybersecurity of products and services and lawful access to data both stem from legal obligations and must be able to coexist***. Lawful access requirements must be implemented on the basis of clear standards developed by all relevant stakeholders (including representatives of industry, data protection and cybersecurity experts, and law enforcement practitioners), reflecting the relevant legal requirements and on the basis of duly assessed potential solutions, thus ensuring that lawful access does not impair the security of products and services.

Many companies and service providers are hesitant to cooperate with law enforcement due to the legal uncertainty associated with voluntary measures and the risk of potential backlash from their users. This reluctance hinders investigations. Moreover, the perception that users prioritise privacy over public security may make industry players reluctant to open channels of communication with LEAs and create adapted mechanisms guaranteeing lawful access. A clear legal framework for lawful access to data is needed to address this issue. Under existing legislation, there are significant obstacles that complicate the provision of such access, especially on a voluntary basis.

Cooperation between companies and law enforcement is inadequate and deficient and needs to be supplemented by clear rules. ***Without clear and enforceable legal obligations, companies are often unable to assist law enforcement in accessing data***.

In the absence of effective solutions to ensure lawful access, ***vulnerability-based solutions are often considered the only option***.

When intercepted data (and potentially other data extracted from a device) is processed by tools designed by private companies, whatever assurances those companies may provide, national authorities have no real visibility on what data is screened and how, and are obliged to rely solely on certificates provided by the government of the country where the companies providing the interception service are based. The need to keep the vulnerability used a secret to maintain the effectiveness of the tools/services exacerbates this problem. This issue is particularly concerning when the provider is based outside the EU.

Last but not least, private companies providing services for intrusive investigative techniques have an incentive to maximise their profits and may therefore decide to sell their tools to regimes that are not democratic (as was the case in the Hacking Team scandal[16]).

Alternatively, challenges in accessing data may ***drive law enforcement to adopt more intrusive investigative measures***. In such cases, LEAs are compelled to resort to more privacy-invasive measures, such as physical surveillance instead of accessing geolocation data, and house searches instead of lawful interception.

Law enforcement authorities' inability to access data can lead to a significant loss of public trust in the justice system. When investigations are delayed or compromised, citizens may perceive the system as ineffective. This erosion of confidence can undermine law and order and diminish the public's willingness to contribute to law enforcement efforts.

Ultimately, ***lawful access enables law enforcement to gather evidence in order to bring justice to victims and protect them from further harm***. Data can provide important leads for uncovering and prosecuting all kinds of crimes, offline and online alike. Individuals can be exposed to severe forms of cyberbullying, identity theft, fraud, etc. resulting from the criminal abuse of digital technologies, services and communications. These experiences can have severe emotional and mental consequences for the victims, exacerbating existing inequalities and vulnerabilities.

[16] See https://www.cbsnews.com/news/italy-hacking-team-breach-suggest-spy-software-sold-fbi-russia-vatican/.

In any criminal investigation, evidence is needed to identify the perpetrator or to demonstrate their responsibility before a judge. It can also help exonerate a citizen if they have been wrongly accused. If investigators and prosecutors cannot access the necessary information, they might not be able to advance their investigations and identify the perpetrator, causing additional distress and financial losses to the victim and eroding trust in the justice system. Traditional physical evidence alone is not always sufficient to establish links and find leads. ***Law enforcement and the judiciary must be fit for the digital age. Only then will they be able to fully shield our societies and economies*** from the growing threats stemming from cyberattacks and hybrid threats, as well as from organised crime activities.

In conclusion, if LEAs cannot access data effectively, their ability to ensure security and apprehend the perpetrators of the most serious offences is significantly weakened. ***Law enforcement should be granted lawful and strictly controlled effective access to data, with robust privacy protection and cybersecurity guarantees, to prevent, detect, investigate and prosecute crimes, thus allowing them to ensure security and allowing EU citizens to live their lives safely and obtain justice for crimes committed against them***.

Chapter I: Digital forensics

WHAT ARE THE ISSUES?

Digital forensics refers to the collection, analysis and preservation of digital evidence (both communication metadata and content data) stored in any digital form on an electronic device, including information from computer hard drives, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, data stored in the cloud and other digital devices.

As difficulties in accessing communication data grow, extracting information from seized devices (or from networks of connected devices) becomes increasingly important to criminal investigations. Accessing data at rest in devices can provide law enforcement with better quality information regarding, for example, identities of members of organised crime groups than other techniques such as lawful interception. Some experts argue that it is not possible to know in advance which data is important for a specific investigation: even information that may seem initially irrelevant could turn out to be vital as an investigation progresses. Access to all data contained in a device may also be important to confirm a suspect's innocence and protect the rights of a defendant[17]. Moreover, investigative methods must always be proportionate.

The chronic **lack of resources** and capabilities faced by LEAs in this area is aggravated by the deployment of new technologies (e.g. new types of devices, IoT and cloud computing), which require new skills and tools. Even if substantial expertise in digital forensics is already available in Member States' agencies and institutions, that knowledge is scattered, and no clear mechanisms exist for sharing and disseminating capabilities, meaning it remains confined in separate silos.

[17] An expert mentioned a case in which a device activity analysis was instrumental in proving that the suspect could not have been involved in a murder.

Digital forensics laboratories' lack of comparable capacities and the general lack of **standardised forensics procedures** and of mechanisms enabling the **recognition of skills and expertise of digital forensics experts** risk hampering cross-border cooperation.

The HLG experts have been clear: **encryption** by default of data on devices is a core challenge that LEAs encounter. Data stored on certain types of modern devices protected by crypto chips[18] or protected by strong encryption algorithms and complex passwords cannot be accessed by LEAs, even using the most powerful decryption platforms. Encryption and other cybersecurity and privacy measures are necessary to protect information systems and communication and personal data, but these measures – and in particular the increasing use of encryption by default – reduce the ability of law enforcement to gather evidence.

Member States have limited **expertise and capabilities** in this field: almost all of them indicate that they lack the technical solutions to meet the needs of practitioners, and the vast majority consider their skills and financial means to be insufficient. LEAs' capacities to decrypt information stored on seized devices vary considerably from one Member State to another, ranging from a success rate of 15-20 % in some cases to more than two thirds in others. Where capabilities exist, they are usually ineffective when it comes to decrypting data that has been secured by strong passwords and files safeguarded in special encrypted containers. Even in cases where decryption is successful, it is often not done in a timely manner. Decryption equipment is expensive and highly specialised, and the hardware is capacity consuming.

Most law enforcement digital forensics departments rely on commercial solutions to access data on devices, which creates additional challenges: these solutions struggle to keep pace with technological developments and quickly become obsolete; the high cost of licences significantly reduces the number of authorised users; and such solutions are often developed outside Europe and may be ill-adapted to the needs of EU LEAs or may not meet EU digital forensics accountability standards.

[18] Such as the T2 security chip on recent Apple laptops.

Often, LEAs have no option other than to exploit **vulnerabilities** to gain access to decryption keys on devices. However, investigative techniques based on this approach need to be reconciled with the objective of ensuring safer hardware and software, as enshrined in the Cyber Resilience Act; vulnerability management and disclosure schemes would alleviate the unintended consequences of such techniques. The experts have considered alternative solutions, such as obliging suspects to hand over to investigating authorities those elements necessary to access relevant devices (e.g. passwords). National legal frameworks applicable in such cases vary significantly, and only three Member States have indicated that they have specific legislative provisions obliging a suspect to provide access to encryption keys or to the decrypted data[19]. Some Member States impose obligations on suspects to make certain biometric data (e.g. a fingerprint) available, thus granting access to a device; in other cases suspects must disclose their password. In general, this remains an area requiring further evaluation.

Some of the issues identified above may be mitigated by **mutualising Member States' capacities** while respecting their exclusive competence in matters of national security. However, this solution remains neglected, sometimes due to legal constraints (in seven Member States there are limitations on sharing tools, while five of them identified limitations in making use of tools shared by other Member States), but more broadly because of the lack of established mechanisms for sharing tools or jointly purchasing licences.

In the past, LEAs used to have clear **channels of communication with manufacturers, providers and suppliers**. This allowed them to establish cooperation protocols which in turn gave them a better understanding of newly implemented technological developments and, as a consequence, facilitated law enforcement action while also ensuring cybersecurity. Given the pace at which new technologies are deployed and new companies enter the market, conditions have changed and cooperation with industry is no longer present.

The adoption of appropriate standards could allow product protocols and technical architecture to be shaped in such a way as to ensure that law enforcement's concerns and technical requirements are taken into account at an early stage. However, **law enforcement's participation in relevant standardisation bodies** is not sufficient, which affects their ability to participate effectively in the development of future technological standards.

---

[19] Eurojust Cybercrime Judicial Monitor (Issue 4), December 2018, p. 34, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_cybercime_judicial_monitor_4_2018.pdf.

POSSIBLE SOLUTIONS

I. Increase and rationalise efforts to enhance capacity in the area of digital forensics tools

Member States already have the expertise and the capacity to perform digital forensics; however, by sharing and mutualising their technical solutions, relevant national institutions and authorities can benefit from other agencies' experience and achieve significant economies of scale, hence reducing the financial resources needed. Member States can further explore solutions to this end, both in the area of digital forensics tools and as regards training and skills development.

Recommendation Cluster 1

To enhance cooperation and build a stronger collective capacity in the area of digital forensics, the experts recommend:

1. *mapping and connecting existing digital forensics networks and establishing a secretariat [recommendation 1];*
2. *making knowledge more accessible and disseminating it among experts [recommendation 1];*
3. *reflecting on mechanisms for pooling knowledge [recommendation 2];*
4. *increasing funding for research and development, with clear deliverables [recommendation 4];*
5. *promoting the Europol Tool Repository as a central hub for the sharing of tools [recommendation 4];*
6. *facilitating the sharing of solutions and digital forensics tools among Member States in an environment of trust (whilst taking into account national rules) [recommendation 2];*
7. *developing a mechanism at EU level for jointly purchasing licences for digital forensic tools, in order to share them among Member States [recommendation 3];*
8. *fostering cooperation with producers and developers of digital forensics tools in order to streamline the structure and format of data obtained by LEAs through use of those tools, ideally following agreed standards [recommendation 12];*
9. *creating a mechanism/scheme for the evaluation and, where relevant, certification of commercial digital forensics tools at EU level, being mindful of any potentially negative impact on investigations and prosecution, such as adding unnecessary burden [recommendation 5].*

Several organisations, networks, associations and projects bring together practitioners and various categories of partners to enhance the capacity of EU law enforcement in the area of digital investigations:

- the *European Network of Forensic Science Institutes* (ENFSI)[20] is the main European network covering (among other topics) digital forensics; it has 73 members from 39 countries, and these members participate in working groups on, for instance, forensic information technology and digital imaging;

- the *European Anti-Cybercrime Technology Development Association* (EACTDA)[21] brings together LEAs, research and technology organisations, industry partners and academia from many Member States, with the aim of facilitating the uptake of security research project results and delivering fully tested and operation-ready software tools, with no licence costs and access to the source code for EU public security organisations;

- the European Anti-Fraud Office (OLAF) has been offering dedicated *Digital Forensics and Analysts Training (DFAT)* since 2007 to national LEAs, with a special focus on fraud, corruption and other illegal activities affecting the financial interests of the European Union; around 175 digital forensics experts are trained per year, thus building a solid community in this area of crime;

- other projects, such as *CYCLOPES*[22] and *iLEAD*[23], are not permanent structures but nevertheless bring together experts and deliver relevant gap analysis.

However, existing permanent networks fall short of bringing together digital forensics units from EU LEAs, as well as organisations that work in close cooperation with them (for instance, the Centre for Cybersecurity and Cybercrime Investigation of University College Dublin (UCD), or the Lithuanian Cybercrime Center of Excellence for Training, Research and Education).

---

20 https://enfsi.eu/.
21 https://www.eactda.eu/index.html.
22 https://www.cyclopes-project.eu/.
23 https://cordis.europa.eu/project/id/740685/en

Europol (in particular the Europol Innovation Lab, together with the European Cybercrime Centre) already cooperates to some extent with all the networks listed above and has demonstrated an ability to bring together a significant number of practitioners, for instance in the form of the Core Groups of the European Clearing Board for Innovation (EuCB), organising the *Forensics Experts Forum*[24] and putting experts in contact with relevant partners, for example through the *Cyber Innovation Forum*[25].

Europol also offers a ready-made infrastructure – the Europol Platform for Experts (EPE) – that enables cooperation and knowledge-sharing among experts on specific topics.

Key action: HLG experts call for Europol's digital forensics capabilities to be enhanced

Actors: Europol, European Commission, Member States,	*Time: 2028*	*Budget: to be discussed at a later date depending on the outcome of the ongoing discussions on the next MFF*

- As part of the considerable reinforcement of Europol announced in the Political Guidelines for the 2024-2029 European Commission, the HLG experts call for a strengthening of Europol's capacity to help Member States to **pool resources, knowledge and expertise and to share solutions and digital forensics tools** in an environment of trust. Sovereign tools and those used and/or developed exclusively for national security purposes should be excluded.
- The HLG experts call on Europol to **play the role of a hub** for access to relevant operational expertise in the field, and possibly to **set up a project similar to SIRIUS in the area of digital forensics** to facilitate the sharing of knowledge and expertise and the exchange of best practices.
- The HLG experts call on Europol to step up its role in **coordinating organisations and projects** that contribute to the creation of knowledge in the area of digital forensics at EU level, under the guidance of the EuCB and taking into account the input of other relevant agencies.

[24] https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference
[25] https://www.europol.europa.eu/publications-events/events/ec3-cyber-innovation-forum-2024

Several financial instruments exist to support research and tool development in the area of digital forensics.

- Under the *Internal Security Fund (ISF)*, the European Commission periodically publishes open calls for proposals in the area of cybercrime and digital investigations. Despite the rather limited budget (under the current MFF, around EUR 15 million has been allocated to these actions), projects selected under these calls have proven to be targeted and successful.

  Roughly two thirds of the ISF budget is allocated through shared management, with Member States choosing which projects to finance and taking responsibility for day-to-day management. Hence, Member States have the possibility of supporting projects on digital forensics in the framework of their respective National Programmes.

- With a total budget of EUR 1 694.6 million over seven years, *Horizon Europe Secure Societies* aims to foster secure European societies in a context of unprecedented transformations and growing global interdependencies and threats, while strengthening the European culture of freedom and justice. In recent years, it has supported several relevant research projects, such as FORMOBILE[26] and EXFILES,[27] which have supported practitioners in their day-to-day activities.

- The *Digital Europe Programme* is the main EU funding instrument aimed at enhancing the EU's digital infrastructure through a variety of initiatives. The programme, which has a total budget of EUR 7.5 billion for the period 2021 to 2027, allocates significant resources specifically to cybersecurity, and also covers digital forensics.

[26] FORMOBILE – From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices: https://cordis.europa.eu/project/id/832800.

[27] EXFILES – Europe fights against crime and terrorism: https://exfiles.eu/.

The Europol Decryption Platform is a flagship project under the ISF. Set up by Europol in 2020, in close cooperation with the European Commission's Joint Research Centre (JRC), this platform supports national LEAs by decrypting their digital evidence. It aims to provide a sustainable solution for LEAs to access the technical and IT resources they need. Over the past few years, the platform has been used in numerous major cases and produced instrumental results in nearly half of them, leading to several success stories. In 2023, the platform successfully supported 37 investigations (into child sexual exploitation, terrorism, cybercrime, organised crime, drug smuggling and fraud, as well as high-profile financial investigations), including high-priority investigations such as those into SkyECC and Encrochat. The platform has become an essential tool for LEAs, but it is not sufficient to address all the issues related to decryption encountered by EU authorities.

Key action: HLG experts call for the use of EU decryption capabilities to be further developed and fostered

Actors: European Commission, Europol	*Time: 2028*	*Budget: to be determined by Member States (e.g. under ISF national programmes)*

- The HLG experts call on the European Commission to support national authorities' ability to gather high-quality contextual information, while respecting Member States' exclusive competence in matters of national security, through dedicated funding (for instance under the ISF National Programmes) and best practice exchange, so that they can contribute to boosting the efficiency of the Europol Decryption Platform.
- The HLG experts call on the European Commission to support Europol's investment in maintaining technical capabilities and enhancing decryption capabilities, keeping pace with technological developments and factoring in research on quantum cryptography.
- The HLG experts call on the European Commission to financially support Member States in developing **national and regional decryption capabilities**, to complement Europol's efforts.

The existing EU funding programmes offer significant support to law enforcement. Further streamlining these opportunities would increase their contribution to improving digital forensics departments' capacities and decreasing vendor lock-in and law enforcement reliance on 'black box' tools (i.e. tools which process data without trusted authorities being able to verify how they function) developed outside the EU.

The steps in the cycle of activities (research, development, uptake) that should be taken to deliver tangible added value to LEAs are supported by different schemes. To fully reap the benefits of the opportunities available at EU level, national administrations, LEAs and practitioners should be aware of the functions and objectives of each specific programme and mechanism.

Horizon Europe has supported various successful projects, with the active participation of law enforcement practitioners. However, Horizon Europe is a research programme and expectations regarding how close the tools developed are to being ready to be operationally deployed should be adjusted.

The project *Tools4LEAs*, funded by the ISF and run by the EACTDA, aims to facilitate the uptake of security research project results and deliver fully tested and operation-ready software tools, with no licence costs and access to the source code for EU public security organisations. *Tools4LEAs* is best placed to build on results of research projects to help deliver operational tools. Europol is involved in the *Tools4LEAs* project and – together with all end-users that are members of the EACTDA – steers its work.

The EuCB has created more than 15 Core Groups of Member States to exploit new technologies and co-create innovative tools together. Member States have used EuCB Core Groups to coordinate part of the development of innovative tools financed by ISF grants, such as MARIT-D, ProfID and web crawlers. Core Groups are an ideal framework through which Member States can coordinate the co-creation of digital investigation tools.

Through targeted *calls for proposals under the ISF*, the European Commission continues to fund projects which have significantly contributed to the success of operational actions. For instance, the CERBERUS project located the vulnerabilities in the EncroChat system that would allow the French Gendarmerie, supported by the Dutch National Forensic Institute and UCD, to dismantle it. The FREETOOL project[28], meanwhile, led by the UCD Centre for Cybersecurity and Cybercrime Investigations, enabled the development of a range of free cybercrime investigation tools[29], tailored to meet specific law enforcement requirements in digital investigations and analysis. These tools were developed in partnership with law enforcement and are freely available to the law enforcement community. 3 000 users from over 100 LEAs spread across dozens of jurisdictions have signed up for access to the tools, which have also been adopted at an organisational level by several LEAs and used in high-profile investigations. The *Justice Programme* also covers judicial cooperation in criminal matters and could potentially promote cross-border cooperation on the use of digital investigation tools.

28 https://www.ucd.ie/cci/projects/freetool/.

29 The tools cover the various phases of an investigation: pre-search open source intelligence (OSINT) gathering; live data forensics; memory analysis; post-search OSINT and online resource preservation; automated file/artefact retrieval; forensic reporting; media processing; geolocation of artefacts; and media comparison with cross-case media matching.

Since its creation, the *Europol Tool Repository* (ETR) has evolved to encompass over 40 advanced tools providing direct access to state-of-the-art technologies for European law enforcement. New tools are added every month, and the repository has become the primary source for EU practitioners looking for software to aid their investigations. ETR currently has more than 2.7K users, and more than 7.8K downloads of its various tools. The tools have been widely used by national investigative units in support of multiple operations, including in the various crime areas, such as trafficking in human beings, serious and organised crime, cybercrime and online child sexual abuse. ETR offers a direct exploitation opportunity for EU-funded projects that offer concrete and mature results and whose creators are willing to license them to Europol for dissemination to all European LEAs. Selected partners from the INSPECTr, Tools4LEAs and FORMOBILE projects have already shared tools in ETR. Europol is coordinating with the EU Agency for Law Enforcement Training (CEPOL) to offer user training on ETR tools.

Moreover, the Digital Europe programme should increasingly foster synergies and complementarities between cybersecurity and fighting cybercrime, which often rely on the same digital forensics tools and techniques.

At present, no mechanism exists to ensure that digital forensics tools comply with accountability and forensic standards within the EU. Such a mechanism should provide for a technical evaluation ensuring that proportionality (i.e. providing proof that the tool allows access to targeted information, hence limiting the analysis solely to what is necessary), transparency and the rights of the defendant (i.e. demonstrating that the tool retrieves information that is authentic and accurate, hence providing assurance to defence lawyers and to independent forensics experts testifying in court) and other legal requirements (e.g. compliance with the AI Act) are fully respected. This would boost the trustworthiness of the evidence in court, at national level as well as across borders, hence strengthening cross-border cooperation.

Key action: HLG experts call for targeted funding for projects for research into and development and uptake of digital forensics tools

Actors: European Commission, Europol, Member States, EACTDA, ENFSI	*Time: as of 2024*	*Budget:*

- The HLG experts call on Member States to **integrate digital forensics projects funded under their respective ISF National Programmes within existing mechanisms** (e.g. EMPACT) or networks (e.g. ECTEG, EACTDA), in order to benefit from the experience of practitioners from other Member States and at the same time promote the dissemination and uptake of results by other LEAs.
- The HLG experts welcome the ongoing efforts of the European Commission to support the research, development and deployment of digital forensics tools through funding under relevant financial programmes: **Horizon Europe**, **Digital Europe** and the **ISF**. Depending on available resources, every two years, the European Commission will publish **open calls for proposals** in the area of cybercrime and digital investigations, under the ISF.
- The HLG experts welcome the ongoing efforts of the European Commission to fund the **EACTDA** under the ISF, so that the EACTDA can deliver fully tested and operation-ready software tools with no licence costs and access to the source code for EU public security organisations.
- The HLG experts welcome the ongoing efforts of the European Commission to promote, in the framework of funding opportunities, the use of the **Europol Tools Repository** as a central hub for the dissemination of tools; they encourage the **Europol Innovation Lab** to continue its efforts to make trusted, secure, free-of-charge, easy-to-install and scalable investigative tools available to EU law enforcement.
- The HLG experts call for further consideration to be given to the **establishment of schemes for the evaluation and, where relevant, certification** of commercial digital forensics tools at EU level. This may be done, for instance, **in the framework of the European Network of Forensic Science Institutes.**

Licences for digital forensics tools are costly and sometimes unaffordable for some LEAs. Joint acquisition of licences which can then be shared among authorities in different Member States may allow lower prices to be negotiated.

The *iProcureNet* project[30], funded under Horizon Europe, has built a methodology for joint procurement in the area of security, as well as a network of procurement authorities in Member States. Given its composition and the organisation of its work, the *EU Innovation Hub for Internal Security* would be well placed to accompany the definition by Member States of common needs and to identify which tools would be most useful, provided a dedicated digital forensics workstream were created.

Often, digital forensics tools present additional issues beyond their cost. For example, data retrieved by these tools may be structured or presented in a format that does not comply with existing domestic information systems used for further processing (e.g. data analysis or sharing). Hence, it is necessary to formulate a set of Member States' shared requirements regarding the structure and format of data obtained through digital forensics tools. On that basis, Member States' authorities would be in a position to engage in discussions with digital forensics tools providers so that their requirements can be taken into due account, for instance in the framework of joint procurement procedures, as outlined above.

Key action: HLG experts emphasise the need for better value for money when acquiring digital forensics tools

Actors: Member States, European Commission, EU Innovation Hub for Internal Security, Europol	*Time: as of 2025 (joint procurement)*	*Budget: N/A*

- The HLG experts call on the European Commission to:
  - support Member States in **identifying the digital forensics tools** most needed for effective investigations (possibly in the framework of the EU Innovation Hub for Internal Security) ;
  - support **cooperation between operational units and the contact points in procurement authorities,** brought together by iProcureNet;
  - set up **pilot joint purchases of digital forensics tools licences**.
- The HLG experts believe that **Europol** is in a position to assist Member States in defining **common requirements regarding the structure and format of data obtained** through digital forensics tools and, on that basis, foster cooperation among relevant national authorities and experts to allow them to engage with producers and developers of those tools so that they can agree on standards and Member States' requirements can be taken into due account.

[30] https://www.iprocurenet.eu/.

II. Exchanging capacities and sharing sensitive tools

At present, the exploitation of vulnerabilities to access decryption keys on devices remains the main option left to law enforcement to access encrypted content, given the limited availability of decryption capabilities (e.g. Europol Decryption Platform) and the absence of effective cooperation with industry or a dedicated legal framework to ensure lawful access to information on digital devices.

Even if (some of) these conditions may be in place to some extent, criminals are likely to rely on dedicated encrypted devices to hide information or illegal content. Hence, the need for law enforcement to use and possibly share sensitive tools[31] and capacities will persist in the foreseeable future.

Recommendation Cluster 2

To share sensitive tools and the responsible management of related capacities, the experts recommend:

1. *reflecting on the establishment of mechanisms to ensure that sensitive tools can be shared in a way which fully respects national rules [recommendation 1];*
2. *setting up a process dedicated to the exchange of capacities that potentially involve the use of vulnerabilities, which would allow knowledge and resources to be pooled while ensuring that the confidentiality and sensitivity of the information would be respected [recommendation 6];*
3. *possibly exploring a European approach to the management and disclosure of vulnerabilities handled by law enforcement, based on existing good practices [recommendation 2].*

Through Horizon Europe and the ISF, the European Commission has supported projects (*EXFILES* and *ForRES*[32]) dedicated to vulnerability and software exploitation, providing law enforcement practitioners with tools and protocols for rapid and consistent data extraction which nevertheless complies with all relevant legal provisions.

---

31 'Sensitive tools' refers to both digital forensics and tactical interception tools.

32 https://forres.eu.

Sharing sensitive tools and related capacities among trusted European partners facilitates operational cooperation, allows for mutualising knowledge and creates economies of scale, reducing the necessary resources.

Though it is still sometimes key to investigations, the exploitation of vulnerabilities must be handled with extreme care, in compliance with the relevant domestic legal framework, as it impinges on the security posture of hardware and software.

Key action: HLG experts call for support in sharing sensitive tools and the responsible management of related capacities

Actors: Member States, European Commission	*Time: as from 2024*	*Budget: N/A*

- The HLG experts invite the European Commission to continue to support projects dedicated to the sharing of sensitive tools (both digital forensics and tactical interception tools) and the pooling of resources through relevant funding programmes; the Commission could also support the **creation of a transnational platform for structuring and sharing knowledge**.
- The HLG experts invite the European Commission's JRC to explore the feasibility of setting out a **European approach for the management and disclosure of vulnerabilities**, handled by law enforcement, based on existing good practices

III. Collective investments to develop skills and enhance expertise in the area of digital forensics

Relevant law enforcement staff should be trained to use investigative tools and techniques applied in their investigations, and their expertise should be certified. Their required and documented competences should reflect their role and include at a minimum generic mobile device digital forensics (tool-agnostic), chain of custody/evidence topics, and basics about types of acquisition, analysis, reporting and court appearance. Documentation should reflect whether these competences are acquired through training or on the job.

Recommendation Cluster 3

To support the development of skills and expertise in the area of digital forensics, including decryption and standardisation, the experts recommend:

1. *increasing the number of training opportunities for experts [recommendation 7];*
2. *creating a certification scheme at EU level for digital forensics experts, to guarantee the quality and uniformity of technical training provided [recommendation 7];*
3. *investing to fill the gap in technical skills in standardisation and increasing awareness by establishing agreements with academia and other relevant institutes [recommendation 8].*

CEPOL delivers training courses on several relevant topics[33]. The European Cybercrime Training and Education Group (ECTEG)[34] develops courses on cybercrime and digital forensics and makes them available, free of charge, to CEPOL and to national LEAs.

ECTEG has developed *Decrypt*, a training resource to enhance EU Member States LEAs' lawful decryption capacities through sophisticated strategies for handling encrypted evidence in a lawful manner. Decrypt can be deployed by CEPOL, as well as national units, making use of the infrastructure made available by the JRC.

[33] Digital forensic investigator training, mobile forensics, live data forensics and Mac forensics.

[34] ECTEG is a not-for-profit organisation which brings together 30 LEAs from 20 European countries, international bodies and academia. With the support of the ISF, ECTEG develops, promotes and shares training resources, solutions and materials. See https://www.ecteg.eu/.

It is equally important to provide first responders with basic skills concerning digital forensics. Among other projects, ECTEG has created *eFirst (*'Educating law enforcement first responders on cyber-essentials'*)*. eFirst is an online, self-paced training module aimed at police officers in the field (patrol, crime scene, house search) or tasked with taking a victim's initial complaint. It provides basic knowledge about cybercrime and digital forensics. It can also be used as a basis for in-person courses at police academies.

Certification of experts' profiles ensures that each person has the necessary knowledge and skills. It motivates professionals to develop their skills and stay up to date on developments in their field, and it also supports career advancement and personal recognition. This leads to higher-quality and more accurate work. Moreover, personal certification can:

- provide a clear and transparent description of digital forensics experts' skills and competences, enabling practitioners, as well as unit managers, to identify who they need to meet the necessary requirements for the efficient handling of relevant tasks;
- facilitate the development and steer the organisation of training courses at national, regional and EU levels; comparable police training across all EU Member States ensures that all police officers have access to a consistent level of knowledge and skills, irrespective of the country they are from;
- contribute to more transparent judicial proceedings;
- increase trust between investigators and other actors, therefore strengthening international cooperation between national LEAs.

CEPOL has started developing a *Sectoral Qualification Framework* for policing, focusing on cross-border cooperation. This model can be operationalised building on the work that ECTEG has carried out on the certification of digital forensics experts in the framework of its *Global Cybercrime Certification Project*[35].

Both ECTEG and EACTDA are investing part of their resources in supporting effective *participation of relevant law enforcement practitioners in standardisation processes*, for instance by facilitating the acquisition of necessary skills.

Key action: HLG experts call for the enhancement of technical skills and certification of profiles

Actors: CEPOL, ECTEG	*Time: actions ongoing; certification scheme for digital forensics experts to be delivered by 2026*	*Budget:*

- The HLG experts call on CEPOL to continue to **deliver** training courses (especially train-the-trainers courses).
- The HLG experts call on ECTEG to continue to **develop, update and pilot** training courses on digital forensics, for experts and first responders, with particular focus on decryption.
- The HLG experts welcome the ongoing efforts of the Commission (through open calls for proposals under the ISF) to support ECTEG, as well as the **deployment** of training courses at regional level.
- The HLG calls on ECTEG to continue to explore the possibility of putting in place a certification scheme at EU level for digital forensics experts, and on CEPOL to contribute to this effort as much as possible, building on their work on a **Sectoral Qualification Framework** for policing and on **Global Cybercrime Certification**.
- The HLG calls on ECTEG to continue to facilitate the acquisition of **competences and expertise regarding standardisation processes** by relevant practitioners.

[35] https://www.ecteg.eu/running/gcc/.

IV. Facilitating lawful access

Without norms regulating lawful access by design, LEAs must increasingly resort to exploiting vulnerabilities to gain access to seized devices on which information is protected by encryption. However, while this method can advance investigations, it comes at a high financial cost. It is therefore necessary to reflect on possible alternatives.

Recommendation Cluster 4

To establish mechanisms for cooperation with relevant industry partners and explore the possibility of imposing binding standards and approximating legislation in the area of lawful access in compliance with case-law of the Court of Justice of the European Union (CJEU) European Court of Human Rights, the experts recommend:

1. *developing a platform (SIRIUS or equivalent) for sharing tools, best practices and knowledge on how to be granted access to data by product owners, producers and hardware manufacturers [recommendation 11];*

2. *mapping law enforcement points of contact within digital hardware and software manufacturers [recommendation 11];*

3. *conducting comprehensive mapping of and developing an EU handbook on the existing legislation in Member States, in order to detail the legal responsibilities of digital hardware and software manufacturers to comply with data requests from law enforcement, taking into account specific scenarios and requirements that compel companies to access devices; [recommendation 25];*

4. *establishing a research group to assess the technical feasibility of built-in lawful access obligations (including for accessing encrypted data) for digital devices, while maintaining and without compromising the security of devices and the privacy of information for all users, as well as without weakening or undermining communications security [recommendation 26];*

5. *depending on the aforementioned mapping, developing binding industry standards for devices brought to market in the EU, with a view to integrating lawful access and promoting the approximation of legislation within this area [recommendation 25].*

Law enforcement's current engagement with industry is not conducive to concrete results; reinforcing cooperation with industry is needed to develop lawful access pathways to devices and applications for LEAs. For example, in the case of video surveillance recordings, LEAs are increasingly faced with encrypted files that cannot be analysed by automatic software, especially when large quantities of video are involved.

In theory, LEAs may ask for support from device manufacturers, who may in turn provide the source code of their software to make access to content data in clear easier or provide the technical documentation of equipment encountered in criminal investigations.

Europol would be well placed to gather best practices (such the establishment of points of contact for law enforcement) and knowledge on how product owners, producers and hardware manufacturers could facilitate access and make it available to all LEAs through SIRIUS (or an equivalent platform).

In parallel, more transparent solutions enabling access to data in clear on seized devices should be considered, to increase the effectiveness of investigations and, at the same time, ensure a level playing field among industry players, while preserving cybersecurity and safeguarding privacy.

On the basis of a detailed analysis of law enforcement requirements for lawful access, the experts urge the European Commission to draw up a *technology roadmap*[36] that brings together actions by technology, cybersecurity, privacy, standardisation and security experts and ensures adequate coordination.

A key action under this technology roadmap would be to assess the *technical feasibility of built-in lawful access obligations* (including for accessing encrypted data and encrypted CCTV recordings) for digital files and devices[37], while ensuring strong cybersecurity safeguards and without weakening or undermining communications security. This assessment would be carried out involving all relevant stakeholders.

---

36 The report refers to a unique 'technology roadmap' in several instances and chapters.

37 See 'Moving the Encryption Policy Conversation Forward' - Carnegie Endowment for International Peace - https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward?lang=en.

To the extent to which such an assessment confirmed the availability or feasibility of built-in lawful access obligations meeting the conditions above, the technology roadmap should also define the process for a sustained, long-term *engagement with standardisation bodies*. Law enforcement participation in this standardisation process could be coordinated by Europol, with the support of EACTDA.

On the basis of a mapping of existing Member States' legal frameworks determining the responsibilities of digital hardware and software manufacturers regarding compliance with data requests from law enforcement, it would be possible to assess the need for *legislation or guidelines and recommendations* [promoting the approximation of legislation within this area].

Key action: HLG experts call for cooperation with industry to be stepped up, reference to relevant standards in upcoming EU initiatives to be fostered and legislation in the area of lawful access to be approximated in compliance with the case-law of the CJEU and the European Court of Human Rights

Actors: Europol; European Commission | *Time: As from 2025* | *Budget: N/A*

- The HLG experts call on the **European Commission** to develop a dedicated **technology roadmap** to explore options for lawful access to digital devices.
- The HLG experts call on **Europol** to gather best practices and knowledge on how product owners, producers and hardware manufacturers could facilitate access and make it available to all LEAs through **SIRIUS** (or an equivalent platform).

Chapter II: Data retention

WHAT ARE THE ISSUES?

Where, in the past, the primary form of evidence collected was physical evidence, nowadays a huge amount of potential evidence is stored by communication providers in the form of metadata. While digital data is not the only evidence required in the context of criminal investigations, this type of evidence is critical – in particular to establish the identity of suspects or subjects of interest who may have relevant information – in almost all investigations, whether they relate to crimes committed in the physical or in the digital world. Especially as regards the latter, communication metadata (notably IP addresses and port numbers) can often be the only way to identify a suspect[38].

For law enforcement to be able to investigate crimes in the digital age, it is therefore necessary that digital evidence is made available in a readable format and accessible, when necessary, with due respect given to appropriate safeguards for criminal proceedings, procedural rights, and privacy and data protection. Data may be retained for business purposes (such as billing and invoicing) or for law enforcement purposes. Data retention can help to ensure that data is available so that competent authorities can access it in the context of criminal investigations and prosecutions. Data retained by providers may be of crucial importance to effectively fight crime, and preserving such data is a precondition for enabling subsequent law enforcement access and ensuring LEAs can carry out investigations[39]. At the same time, the principle of data minimisation laid down in the ePrivacy Directive[40] and the General Data Protection Regulation (GDPR)[41] stipulates that providers should only store (or otherwise process) traffic data as long as necessary for the purposes of the communication itself, for billing or, in specific situations, for the purpose of marketing ECS. Any other storage must be governed by a legal framework meeting the requirements set out in Article 15 of the ePrivacy Directive. This regime reflects the need to balance the fundamental rights to privacy and data protection with the purposes of law enforcement measures.

---

38 Experts discussed several examples of the relevance of digital data in investigations and the number of requests for data. According to one expert, in the last five years all investigations relating to terrorism or organised crime made use of data requested from providers. In 2023, in one Member State, more than 1 300 000 numbers were requested from operators for identification in criminal proceedings, with nearly all of them later validated by the judicial system.

39 For the purposes of this document, 'access to data' is understood as access granted to law enforcement, subject to *ex ante* judicial authorisation when required, for the purposes of criminal investigations and on a case-by-case basis.

40 Article 6, Directive 2002/58/EC.

41 Article 5(1)(c), Regulation (EU) 2016/679

At present, there is no EU legislation regulating data retention. The CJEU annulled the EU Data Retention Directive[42] (DRD) in 2014, highlighting the significant interferences with the fundamental rights to privacy and data protection inherent in [generally and indiscriminately] storing data originally collected by service providers, for law enforcement purposes[43]. As a result, national legal frameworks have undergone changes that have resulted in substantial differences across the EU[44]: while some Member States still have rules in place obliging communication providers to retain certain categories of data for law enforcement purposes, others have implemented changes to meet the criterion of targeted retention of traffic data proposed in the case-law;[45] others, also due to subsequent judgments by national courts, have no specific rules in place on data retention for law enforcement purposes, and rely solely on data retained by companies for business purposes. The conditions for accessing such data depend on the national legal framework applicable and on the type of data (subscriber, traffic or content data). This lack of coherent and harmonised data retention obligations across the EU results in discrepancies between the Member States in the requirements regulating the retention (and duration thereof) of different types of metadata by service providers.

---

42 Directive 2006/24/EC. The Directive obliged EU Member States to adopt measures to ensure that providers of electronic communications services and networks retained traffic and location data and the related data necessary to identify the subscriber or registered user for between six months and two years, in order to allow access by competent authorities for the purpose of investigating, detecting and prosecuting serious crimes, as defined in national legislation.

43 For an overview of the relevant jurisprudence, see: The future of national data retention obligations – How to apply Digital Rights Ireland at national level? – European Law Blog, V. Franssen; Recalibrating Data Retention in the EU - eucrim; Eurojust/EJCN 2024 report. The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU; Cybercrime Judicial Monitor - Issue 6; Cybercrime Judicial Monitor - Issue 9

44 Member States' responses to the annulment of the DRD diverged, with actions initiated at national level increasing the diversity of national data retention systems. According to Eurojust/EJCN data retention report of 2024 (fn 43), 12 countries made changes to their legislation in the period 2018-2022. Respondents replied that these changes were a direct result of the CJEU cases C-746/18, *Prokuratuur* and Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, Joined Cases C-511/18, C-512/18 and C-520/18. 23 out of 27 Member States have data retention rules in place; seven Member States have already introduced targeted data retention rules. For an overview, see Commission Study on the retention of electronic communications non-content data for law enforcement purposes, 2020, p. 39.

45 The Court has developed the concept of targeted retention of traffic and location data in several judgments, deciding that the retention of data can be compatible with EU law if designed around specific targets and for specific purposes. However, the practical application of the criteria suggested by the Court to design such targets has led to difficulties and challenges in high courts in those Member States who attempted it.

In those Member States that do not have data retention obligations, it is difficult or sometimes impossible to identify a suspect or a person who may have relevant information ('subject of interest') in a criminal investigation[46]. The added value of the new e-evidence rules, once in force, would also be enhanced if they were supplemented by data retention obligations, as otherwise there is no guarantee that the information subject to European preservation or production orders (covering traffic data, data requested for the sole purpose of identifying the user, and subscriber data) will be available.

The current circumstances affect both **law enforcement** and **communication providers**, but most importantly, they have an **impact on citizens and victims**, whose right to access justice cannot be ensured if investigations start when data has already been deleted or has not been retained[47].

I. Issues within the jurisdiction of individual Member States

In Member States **where no specific obligations** are in place regarding the retention of data for law enforcement purposes, investigations rely on the data that companies store for their business and commercial purposes besides any other available evidence. Commercial data is subject to providers' internal policies, with companies storing traffic data for different periods (e.g. around 6 months), while location data, which usually does not have business relevance, is often stored for a shorter time. Often, small companies do not store subscriber or communication metadata at all, or keep them for a very short time. As a result, investigations are often a race against time, as investigators need to identify the provider of the data and transmit the request in line with applicable rules before the data is deleted, which is sometimes a matter of days or hours. In some cases, companies do not provide information on the specific data that they process and hold, making it difficult for competent authorities to submit targeted requests when they seek data. Some hosting services allow users to rent server space using fictitious data, meaning that even if they store user data, it is not reliable[48].

---

46 See example reported in Background document Operational challenges faced by law enforcement related to access to data Input to the first plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement, p. 4

47 In the context of impact on citizens and victims, see *Dwyer* v *Commissioner of An Garda Siochána* - [2020] IESC 4 (24/02/2020), in particular para. 9.

48 https://en.wikipedia.org/wiki/Bulletproof_hosting.

In most Member States, legislation on **data retention is in place**. However, as described above, some national legislation has been subject to changes following CJEU rulings that stemmed from the invalidation of the DRD. This has created a diverse landscape, with Member States reacting differently to judgments. In some Member States, efforts have been made to implement a targeted form of retention, which was suggested by the CJEU as a possible way forward on data retention. However, HLG experts stressed that the implementation of such criteria resulted in legal and technical issues with regard to their feasibility[49], and providers criticised the costs related to the technical implementation of targeted retention and, more generally, of frequently changing legislation. Another major legal issue encountered at national level is that national legislation in most cases does not cover OTT services. The specific case of OTT services will be explored more extensively below in section 1.3.

II. Cross-border issues in the EU

Issues related to data retention also occur in relation to cross-border requests, i.e. when a competent authority seeks data from a provider based in a different Member State. In cases involving cross-border requests, authorities in the receiving country may not be able to execute a request (due to the absence of data or of relevant legal rules) issued by another country.

The lack of harmonised obligations on retention of metadata across the EU results in obstacles for law enforcement in one Member State **seeking data** from providers based in other Member States. Even when data retention regimes are in place at national level, there is no coherence between national schemes on retention periods, with these varying significantly from Member States to Member State[50].

---

[49] While the CJEU provides some guidance on and examples of how to construe **targeted retention** of traffic data, case-law can only give indications and is not precise enough to detail possible constraints on the retention of all data categories. As a consequence, several cases against rules on data retention have been brought before the Court in recent years and Member States are not in a position to ensure legal certainty.

[50] Depending on the data and the type of crime, retention of metadata may vary from 6 to 72 months. In the Eurojust/EJCN data retention report of 2024 (fn 43), respondents indicated that less data was available as a result of the lack of retained data, the limitations imposed on the categories of data that can be retained, and short(er) retention periods. The unavailability of data consequently also affects authorities' ability to execute European Investigation Orders and mutual legal assistance requests.

Equally, no harmonised approach exists at EU level on the **definition of the data** that needs to be retained[51]. National legislation may oblige service providers to retain different categories of data for different purposes (taxes, audits, law enforcement). They also differ in the level of detail they provide in this regard, with some legislations providing detailed lists of non-content data to be retained, while others provide broader definitions of non-content data[52]. Depending on the service they offer and their business and commercial needs, providers also retain different types of data for different time periods. This results in a highly varied landscape, with substantial differences existing not only between Member States, but also between services.

Such differences are also relevant because of those existing between Member States as regards accessing retained data too: some Member States require judicial authorisation for access to some types of metadata, while others do not. Service providers report that the legal uncertainty on the rules applicable for disclosing data is one of the causes of delays and of non-compliance with law enforcement requests.

---

51 As reported in the Commission Study on Data Retention (fn. 34 44), p. 48: 'While certain types of information are always classified as subscriber or traffic data across all Member States, there is no consensus on the classification of the following data points: IP addresses, SIM numbers, device identification numbers (e.g. IMSI, IMEI) and port numbers for dynamic IP addresses. In some Member States (EE, FR, IE), these data points are classified as subscriber data while others (DE, ES, IT, PL, SI) classify them as traffic data.'

52 See Commission Study on Data Retention (fn. 44 34), Annex III, for an overview of data retained in each Member State.

Competent authorities need to comply with the national regulations applicable to the provider holding the data sought, but also with the specific requirements set by the providers themselves. As reported in the SIRIUS Annual Report 2022[53], providers may require the use of dedicated portals, or the submission of requests in specific templates or languages. They may also require information on the nature of the case, a clear reference to the national legal basis for the request or the specification of narrow timeframes for the data sought. While some of these issues will be addressed with the implementation of the e-evidence package by 2026, the HLG experts stressed the need for coherence between these rules and any potential harmonised framework on data retention. While standards have been developed by the European Telecommunications Standards Institute (ETSI) for the format of requests for number-based interpersonal communications services (traditional telecommunications) metadata, these are not consistently applied across the Member States by providers. Standards for data transmissions from OTT[54] service providers to LEAs are a work in progress and are not fully implemented. Moreover, service providers are free to decide in what form they collect and store user data, and this results in practitioners receiving raw data in very different forms; this creates a significant burden for law enforcement, who would benefit from streamlined processes, **communication systems and formats** for submitting requests and for sending and receiving replies to requests and data. Standardised communication systems and formats would also reduce the costs of processing requests for companies.

Once law enforcement has gained lawful access to data, they need to be in a position to exploit it; hence, the data needs to be **readable**. However, providers are increasingly offering services which allow traffic data to be end-to-end encrypted, and when they provide this data to law enforcement and judicial authorities upon request, they often provide it in this encrypted form.

Finally, another perceived consequence of this status quo relates to the risk that law enforcement will see their **evidence challenged** in court[55]. The CJEU has clarified that the admissibility of

---

53 sirius-eu-digital-evidence-situation-report-2022, p. 14.

54 In this report, 'over-the-top (OTT) communication services' refer to applications and services that provide communication and media services (such as messaging and voice and video calls) over the internet without the involvement or control of traditional telecommunication service providers (telecom carriers). Common examples of OTT communication services include messaging apps such as WhatsApp, Telegram, Facebook Messenger; voice and video calling services such as Skype, Zoom, Google Meet, Viber; and social media platforms such as Instagram and Snapchat (messaging and media sharing).

55 See chapter 'Collection and admissibility of evidence' in Eurojust/EJCN data retention report of 2024 (fn 43).

evidence obtained by means of data retention is a matter of national law[56], subject to the principles of equivalence and effectiveness[57]; The differences between national data retention regimes may therefore have an impact on the admissibility of evidence in cross-border proceedings[58].

III. Issues related to OTT and other providers

While the above issues pertain to all providers of ECS, OTT providers present additional challenges for LEAs in lawfully accessing data. At both national and EU level, OTT providers often do not consider themselves to be bound by the same obligations as traditional communication providers. While OTT providers fall within the scope of the EECC, the fact that they are often established outside the EU and the absence of licensing systems (i.e. they may be subject to general authorisations only) and sanctions create uncertainty with regard to their obligations to retain data, including specific types of data, and making enforcing compliance challenging. Moreover, while traditional communication providers in most cases retain some data for business purposes enabling the identification of users (such as IP numbers with port number and timeframe), this is not the case for **OTT service providers,** which only retain non-content data needed for their commercial purposes, in some cases for only a short period of time[59]. OTT providers do not retain any non-content data connected to a dynamic IP address (port number and timeframe). This can make it difficult or even impossible to retrieve metadata of communications taking place via systems such as WhatsApp or Telegram, which are increasingly used. As mentioned, the types of data retained also vary depending on the service offered. While in some cases the providers issue guidelines describing the types of data that they retain[60], in other cases, OTT providers do not disclose this information. This, together with the lack of **obligations on transparency** regarding the types of data that providers generate, process and store for business purposes, results in frequent issues for LEAs when they attempt to identify whether data has been retained, who holds what data and what types of datasets can be requested, and ultimately when they send requests to providers.

---

56 CJEU, judgment of 6 October 2020, *La Quadrature du Net and Others*, Case C-511/18, ECLI:EU:C:2020:791 para. 222 – 228; judgment of 5 April 2022, *Commissioner of An Garda Síochána and others*, Case C-140/20, ECLI:EU:C:2022:258, para. 127.

57 Ibid para. 223: '…provided that [...] those rules are no less favourable than the rules governing similar domestic actions (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness).'

58 Several court cases have challenged the admissibility of non-content data as evidence. For a summary, see Commission Study on Data Retention (fn.44 34), p. 41.

59 This is especially the case for small providers. According to the Commission Study on Data Retention (fn 5) p. 103, IP addresses are retained on average for 30 days.

60 See for example law-enforcement-guidelines-outside-us.pdf (apple.com).

At the same time, the increasing volume of requests received by providers[61], paired with the need to process large-volume datasets, contributes to requests being delayed or rejected[62]. In addition to causes stemming from providers' specific business model decisions, this is also due to the **limited number of mechanisms for cooperation** between law enforcement and judicial authorities on the one hand and private companies on the other.

Finally, though they may not fall under the EECC's definition of communication service providers, a number of emerging technologies and other digital players (such as car manufacturers and large language model (LLM) AI systems) generate and handle communication metadata that can provide information on criminal activities. Despite the increasing amount of data these services handle, currently they are not bound by data retention obligations.

POSSIBLE SOLUTIONS

I. Reinforcing cooperation between communication providers and practitioners

In a context where the gathering of digital evidence is impeded by the lack of harmonised rules, LEAs often have to rely on **voluntary cooperation** with service providers to conduct investigations. While this solution has aided certain high-profile investigations[63], it is subject to legal uncertainty and is not always viable: voluntary cooperation depends on the type and size of the service provider, with small ones often retaining data for a very short time compared to bigger ones or not having the resources to respond to LEA requests[64].

---

61 According to the SIRIUS Annual Report 2023, the volume of data requests to service providers is steadily increasing every year (see p. 66 et seq.).

62 SIRIUS Annual Report 2023 (fn 49) provides an overview of the main causes of delay/rejection of requests for electronic evidence (see p. 68 et seq.).

63 See examples in SIRIUS Annual Report 2023 (fn 49), p. 19.

64 In the SIRIUS Annual Report 2023 (fn 49), p. 79, the high volume of requests under voluntary cooperation is reported as being challenging for service providers, and it is recommended that they take part in SIRIUS international events so that 'smaller OSPs can take advantage of the expertise of the SIRIUS Project in the field of cooperation with authorities to increase their understanding of the matter, structure their policies for responding to authorities' requests and ensure that they are prepared for upcoming legislative developments.'

Partnerships and cooperation with industry need to be underpinned by a **clear legal framework,** as an essential component of any viable solution allowing law enforcement and judicial authorities to overcome difficulties in lawfully accessing digital evidence. In addition to both parties meeting their respective legal obligations, it is important that a permanent and trusting relationship is built between law enforcement practitioners and providers, so that they understand one another's needs and can establish workable solutions together. Stable **mechanisms for cooperation** with the private sector are necessary to **increase transparency** on the data that providers generate and store and how long it is retained, but also to ensure **harmonised categorisation of data** to be retained and accessed, to design **standardised formats** for requesting data and to establish **secure channels** for direct exchange between competent authorities and service providers.

Several options for reinforcing such cooperation can be explored, some of them of a binding (hard law) nature, others consisting of soft law solutions. Some of the solutions listed in this section would need to be assessed in the context of the impact assessment referred to in section II and then laid down by law.

Recommendation Cluster 5

To ensure that competent authorities are in a position to seek relevant data by identifying the right data holders, that such requests are received in standardised formats by service providers, and that cross-border cooperation is not hampered by conflicts of law, the experts recommend:

1. *establishing and reinforcing cooperation between law enforcement practitioners and service providers to support the exchange of information, capacity building and training, and to define the principles and modalities of cooperation [recommendation 13], for instance by establishing a clearing house enabling competent authorities to identify relevant service providers and better target lawful requests [recommendation 18]. This could be done:*

    a. *by building on existing EU-level structures such as SIRIUS, European Judicial Network (EJN)/ European Judicial Cybercrime Network (EJCN), EU Internet Forum;*

    b. *through Memoranda of Understanding, making use of best practices established in certain Member States at national level [recommendation 14];*

2. *fostering transparency rules for providers of electronic communications services and other communications services with regard to the data they process, generate or store in the course of their business, and on informing LEAs about what data is available, taking into account limits posed by the confidentiality of investigations by means of cooperation agreements with service providers or, if necessary, by setting mandatory obligations [recommendation 17, recommendation 16];*

3. *developing streamlined processes and formats based on agreed standards for submitting requests to providers and receiving replies in a structured manner [recommendation 15] and promoting within platforms the designation of single points of contact (SPoCs) for processing requests from and contacts with competent authorities [recommendation 36];*

4. *establishing mechanisms to ensure that cross-border requests are targeted to service providers in a manner that is efficient and avoids potential conflicts, taking inspiration from mechanisms for e-evidence and ensuring the coherence of such mechanisms with the rules established by the e-evidence Regulation [recommendation 19].*

There are currently EU structures in place which allow relevant actors to familiarise themselves with tools and best practices. By bringing together law enforcement, judicial authorities and service providers, the SIRIUS project could facilitate the exchange of knowledge and tools related to requests for user data held by providers[65] and, especially thanks to the existing SIRIUS SPoCs network, serve as a platform for direct connection between requesting authorities and providers[66]. SIRIUS could serve as a **central repository** for legal instruments, case-law, formats, etc, as is the case for cross-border e-evidence sharing[67].

As an existing collaborative environment for Member States, the internet industry and other partners, the **EU Internet Forum**[68] could serve as a space where direct contacts and trust could be established at EU level among relevant actors on activities related to access to digital data. It could contribute to the setting up and keeping up to date of an **open catalogue** of the types of data that providers and data handlers collect and process, possibly to be centrally managed by SIRIUS. Such a catalogue would mitigate the current lack of transparency and create more clarity for law enforcement and judicial authorities on what data they can request, as well as acting as a clearing house for identifying who a request should be sent to. Furthermore, in the event that legal obligations are imposed on providers, the catalogue would provide added value in monitoring and assessing the implementation of transparency obligations with regard to the types of data which providers store or otherwise process.

---

65 The SIRIUS SPoC network of experts in lawful data requests promotes best practices and encourages countries to set up their own SPoC. SPoCs are designated persons, units or institutions which centralise, review and submit requests from governmental authorities to service providers. Currently, 36 LEAs from 25 countries are a part of this network.

66 The SIRIUS project serves as a go-to point for obtaining electronic data from service providers based in other jurisdictions. SIRIUS provides a restricted platform for sharing knowledge and best practices for the law enforcement and judicial communities. The SIRIUS project maintains an up-to-date repository of contact details of over 1 000 companies, focused on smaller, hard-to-find or sometimes inaccessible service providers. Competent authorities are therefore able to retrieve multiple addresses in a single transaction, helping them to deal more efficiently with large volumes of complex information. SIRIUS project | Europol (europa.eu).

67 SIRIUS is an EU-funded project that helps law enforcement and judicial authorities access cross-border electronic evidence in the context of criminal investigations and proceedings. Co-implemented by Europol and Eurojust, in close partnership with the EJN, the SIRIUS project is a central reference point in the EU for knowledge sharing on cross-border access to electronic evidence. SIRIUS project | Europol (europa.eu).

68 European Union Internet Forum (EUIF) - European Commission (europa.eu).

Exploiting synergies with the e-evidence package would save costs and resources and contribute to the full implementation of the e-evidence legislation. For example, encouraging LEAs to create or expand the capacity of units acting as SPoCs for (cross-border) data disclosure requests could be extended to requests made at national level, or the requirement to provide training programmes for investigators and first responders. Equally, the efforts currently ongoing in the context of the implementation of the e-evidence package to set up a **digital platform** to allow for direct exchanges between competent authorities and providers could be replicated for the purpose of communication metadata retained based on national legislation.

Member States could consider setting up **Memoranda of Understanding** as instruments to promote cooperation and develop a common understanding between service providers, government and LEAs, in order to support the operation of national laws. Positive examples in some Member States could provide inspiration for how to structure them, involving all relevant actors (companies, agencies, etc.) in order to ensure that all relevant aspects of cooperation are covered (nomination of SPoCs for service providers and LEAs, technical needs, common definition of categories of data to be provided, shared procedures, drafting of standardised request models, data security and data minimisation measures, etc)[69]. As outlined, **standardised protocols** for the collection of data from providers (including OTT service providers) and for data requests from competent authorities would be beneficial for both law enforcement and service providers, which could set up automated mechanisms for providing responses, reducing costs and saving time. Though differences do exist between **national** and **cross-border requests** (under the e-evidence framework) in terms of requirements, the workflows and the channels through which data is requested could nevertheless be developed, as standardisation pertains to the format of the data requested/received. Standardisation bodies like ETSI are best placed to develop such standardised formats. However, the involvement of Member States' law enforcement experts in these processes has been limited so far. For this reason, the existing **European Working Group on Standardisation on Internal Security**, led by Europol and the Commission, could coordinate and foster Member States' participation in such fora. Work could build on existing standards developed by ETSI, which could be extended to cover other data categories[70].

---

[69] Ireland's MoU dated 6 April 2024 is intended to support the operation of the Communications (Retention of Data) Act 2011 (as amended). The Department of Justice has appointed an independent chair, set terms of reference and invited representation from law enforcement and service providers.

[70] TS 102 657: Retained data handling; Handover interface for the request and delivery of retained data and categories of retained data (subscriber, usage, equipment, network element and billing data); TS 103 120: Interface for warrant information (defines an electronic interface between two systems for the secure exchange of information relating to the establishment and management of lawful required action; typically used for lawful interception but can be used for retained data; typically used between, on one side, a service provider and, on the other side, a government or LEA who is entitled to request a lawful action); TS 103 705: Data Structures for Lawful Disclosure (in development; data structures only, no handover interface, no predefined tree structure, service provider defined types and information).

Key action: HLG experts call for the promotion of cooperation and the development of a common understanding between service providers, government and LEAs

Actors: European Commission, Member States, Europol (SIRIUS), Eurojust, EU Internet Forum

Time: tbd

- The HLG experts call upon the **European Commission, Europol** and **Member States** to evaluate ways of promoting and enhancing cooperation between LEAs and private companies, nurturing a permanent dialogue and mutual understanding of operational, technical and business needs. In the context of the impact assessment referred to in section II, the HLG experts also call upon the Commission to consider the development of specific obligations pertaining to transparency in data collection and permanent cooperation structures.

- The HLG experts invite **the European Commission**, **Europol** and **Eurojust** to set up or promote existing platforms for exchanges between LEAs and the judiciary, on one hand, and communication providers, on the other, to compile a catalogue of the data generated and stored by communication providers and data handlers in the course of their business activities, to be managed by SIRIUS.

- The HLG experts invite **Member States** to explore the possibility of setting up cooperation agreements and/or Memoranda of Understanding bringing together service providers, government and LEAs to support the operation of national laws by laying down principles and standard practices together.

- The HLG experts call upon **Europol** and the **European Commission** to make use of the existing Working Group on Standardisation in Internal Security to foster Member States' participation in standardisation fora, so as to contribute to the definition of relevant standards and jointly design protocols detailing procedures for cooperation with service providers.

- The HLG experts invite the **European Commission**, **Europol**, **Eurojust/EJN** and **Member States** to make use of synergies with instruments such as the e-evidence package to build or acquire relevant tools, for instance by extending the use of digital platforms under development to serve as request submission portals.

II. Harmonising minimum rules for the retention of metadata by communication providers and access by competent authorities

Experts largely agree that a harmonised EU framework regulating the retention of metadata for law enforcement purposes is needed. Such a framework would provide standardised solutions, as well as clear and enforceable obligations for communication providers and data handlers with regard to when and how to retain data and under which circumstances to provide access to that data. By defining clear rules on retention and access, this framework would serve the purpose of providing clear safeguards for fundamental rights and essential interests, taking into account the indications of the applicable case-law, as well as clarity on rules applicable to communication providers for retaining and sharing data for law enforcement purposes. Additionally, by ensuring that data is retained, such a framework would support the full implementation of the e-evidence package.

Recommendation Cluster 6

To ensure that digital evidence required to investigate and prosecute crimes is available, that no fragmentation exists between Member States with regard to the rules applicable to retention and to the safeguards pertaining to fundamental rights, in particular privacy and data protection, freedom of expression and the rights of the defendant, including the right to due process, and to ensure legal certainty for both competent authorities, on one side, and electronic and other communications services providers, on the other, the experts recommend:

1. *defining categories of metadata based on the purpose of its use (identifying, locating, establishing or assessing the online activity of a subject of interest) [recommendation 28], to ensure that electronic communications services and other communication services providers retain data sufficient at least to identify a subject [recommendation 27, point (v)];*
2. *establishing minimum retention periods for such data;*
3. *designing conditions for access to retained data [recommendation 27, point (iv)] which differ based on the category of data, the category of crime (e.g. crimes that only happen on the internet) or the threat to victims [recommendation 29];*
4. *designing such legal, regulatory and technical provisions in a way that they ensure full respect for the fundamental rights and freedoms of subjects and that any limitation of those rights is necessary and proportionate [recommendation 27, vi];*
5. *ensuring that the same rules, obligations and safeguards apply to traditional communication providers, OTT services and any other existing or future providers generating and processing data [recommendation 27, points (i) and (ii)];*
6. *ensuring that user data retained for commercial and business purposes is effectively accessible for law enforcement under relevant safeguards (recommendation 31) and that competent authorities are able to read data lawfully received from providers [recommendation 27, point (iii)];*
7. *ensuring that Member States can enforce sanctions against electronic and other communications services providers which do not cooperate with regard to the retention and provision of data, e.g. through the implementation of administrative sanctions or limits on their capacity to operate in the EU market [recommendation 30].*

When talking about **retention of metadata**, distinctions should be made between categories of data, distinguishing the data needed to identify a subject of interest (subscriber data[71] and IP addresses of source communication[72]) from traffic[73] and location data[74], and providing for different retention periods and safeguards for each category. Also at the data access stage, the aim is to ensure a balance between the seriousness of the crime to be investigated and the degree of intrusiveness into privacy of the measures to be taken. In line with recent case-law[75], minimum requirements for generic retention of data sufficient to ensure that any user can be clearly identified could be explored. For traffic and location data, additional and stricter criteria need to be examined.

With the aim of designing such a framework in the most future-proof and **technology-neutral** way possible, the categorisation of data to be retained should be formulated based on a forward-looking approach, including generic datasets based, for example, on the functions of the data (data which allows uniquely identify a communication source or destination, data which allows the location of a communication source to be identified, etc), combined with a list of existing types of data (IP address, IMEI, etc). This framework would allow the intrusiveness of each data category – and hence the safeguards required – to be properly assessed.

---

71 With some exceptions in the case of small providers, user data is generally already retained for business purposes. When this is the case and without prejudice to proportionate safeguards, such data should be made available to law enforcement.

72 The case-law allows the general and undifferentiated retention of data related to the civil identity of users of electronic communications for the protection of public interests and the generic and undifferentiated retention of IP addresses to protect national security, fight serious crime and prevent serious threats to public safety (judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined Cases C-511/18, C-512/18 and C-520/18, and judgment of 30 April 2024, *La Quadrature du Net and Others () and lutte contre la contrefaçon)*, Case C- 470/21 ('Hadopi'), ECLI:EU:C:2024:370).

73 'Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof (Art. 2 of Directive 2002/58/EC).

74 'Location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service (Art. 2 Directive 2002/58/EC); location data of the user's equipment should be considered location data other than traffic data, as defined in Article 9 of Directive 2002/58/EC.

75 Hadopi judgment.

As posited by the experts and the recent case-law[76], combining retention obligations with strict **requirements regarding access to data** would provide additional safeguards for fundamental rights, in particular privacy and data protection. Thus, the HLG experts discussed the need to design access rules which differ depending on e.g. the type and seriousness of the crime, the degree of threat posed to the victims by the offence, the purpose of access and the authorities competent to access the data. Such an approach was also considered a useful way of setting out specific rules for the investigation and prosecution of crimes that are particularly challenging to investigate, such as those committed exclusively on the internet, where digital evidence is the only evidence available.

Once data has been lawfully accessed, the requesting authorities need to be able to read it. Hence, data needs to be provided in an **intelligible format** by providers. Often, providers offer end-to-end encrypted services[77] for traffic and subscriber data, and they do not decrypt this data when they share it with competent authorities. The HLG experts were of the view that a data retention regime should include obligations for service providers to provide data in clear while ensuring strong cybersecurity and full compliance with data protection and privacy law, and without undermining encryption.

Minimum requirements for retention of specific categories of data would need to be applicable (and enforceable) to any (present or future) economic operator providing ECS, to make the data retention framework effective both now and in the future. In order to take into account future technological developments, entities subject to data retention obligations should include telecommunication providers, OTT providers and other operators collecting data connected with a specific individual or legal person who uses their service, such as car manufacturers or LLM AI systems. These obligations must be enforceable, and there must be accountability for providers; this could be achieved using a variety of solutions, which could include market barriers (licences to operate) and administrative sanctions.

---

[76] In the recent Hadopi case, the Court inferred that privacy can be guaranteed by combining retention and access.

[77] See section I.

A system of enforceable sanctions for non-cooperative providers and providers who host illegal services constitutes an essential aspect of any future EU framework. Given the interaction between this specific aspect and the possible solutions discussed in the context of lawful interception, sanctions are to be discussed at the next meeting on lawful interception.

While for most providers, obligations to retain and provide data would require mainly technical implementation (i.e. making data collected or processed for business purposes available to competent authorities), this would entail imposing user registration procedures by default on providers which do not currently register their users because they have no business need to do so (such as OTT providers). Obligations of this kind were considered positive by the HLG experts in the context of the discussions on the need to increase **transparency and accountability** for providers with regard to the data they collect and store, and for how long. Existing obligations for categorisation under other instruments (GDPR) can provide insights on the data processed by these providers.

Key action: HLG experts call for a new EU data retention and access framework

Actors: European Commission, Council, European Parliament

Time: 2025-2026

- The HLG experts urge the **European Commission** to launch the process for an impact assessment to evaluate the different options for enhancing competent authorities' capacity to effectively investigate and prosecute crimes by accessing historical metadata generated and stored by communications providers. The impact assessment should also cover subsidiarity requirements, the impact on fundamental rights and on the internal market, and the relationship with other existing legal instruments. It should serve as a basis for a legislative proposal, to be adopted by means of the Ordinary Legislative Procedure.

Chapter III: Lawful interception

WHAT ARE THE ISSUES?

'Lawful interception of communications' refers to a third party – an authority or another entity empowered by or on the basis of a law – gaining covert access to data from a suspicious communication. While lawful interception in the past was relevant mostly for phone calls, the increasing shift from traditional voice calls to messaging services and other forms of electronic communications has created new challenges.

The EECC recognised this shift and extended part of the legal framework that applies to traditional telecommunications to companies that offer internet-based services over a telecommunication infrastructure that they do not own or manage, including number-independent interpersonal communications services (NI-ICS). In practice, this means that NI-ICS providers can potentially be subject to the same legal framework that has been applicable to traditional telecoms operators, including for lawful interception. Member States can require that operators allow lawful interception of electronic communications by national competent authorities in accordance with Regulation (EU) 2016/679 and Directive 2002/58/EC, which contain the provisions for confidentiality of communications and the exceptions to it. Under the general authorisation regime under the EECC, Member States can restate this requirement.

Lawful access does not need to be at network level – as used to be the case for traditional phone calls and text (SMS) messaging – but can also be on the user's device (before the information is sent) or at destination level (e.g. when messages are stored in the cloud). In the context of this report, lawful interception covers these three use cases and concerns data accessed in real time or with little delay.

It is important to distinguish between interception technologies that are **implemented by a communication operator** and technologies that can be deployed autonomously by LEAs. Only the former [referred to as '**operator-based interception**' in this report], which requires the installation of technical systems by the communication operator to collect and deliver the intercepted data to the requesting authorities, is included in the ETSI standards' definition of 'lawful interception'. The latter [referred to as '**tactical interception**' in this report] refers to tools that do not require permanent physical installation on a network, such as IMSI catchers[78] or software for intercepting data on smartphones. Those use cases imply different levels of intrusiveness and challenges of a different nature and do not fall under the same legal regime.

While lawful interception of traditional telecommunications remains an essential tool in many investigations[79], the effectiveness of this measure has drastically decreased as telecoms services are now mostly provided by other actors: according to various sources, around 97 % of all mobile messages are now sent through messaging apps like WhatsApp, Facebook Messenger, and WeChat, while traditional SMS and MMS messaging accounts for only about 3 % of messages. In addition, in 2023 more than 90 % of OTT communications were carried out through end-to-end encrypted services[80].

Experts agree on the following trends: first, criminals began to move from traditional communication operators to mainstream OTTs; then, progressively, top criminal actors started using dedicated criminal networks (such as Encrochat and Sky ECC); and since 2020, following the disruption of major encrypted criminal communication networks, many of them have decided to move back to regular end-to-end encrypted OTTs.

---

78 IMSI catchers are surveillance devices that mimic cell towers to intercept mobile phone signals, capturing international mobile subscriber identity (IMSI) numbers and communication data.

79 There has been a significant and steady increase in lawful interception requests in Europe in recent years. Countries like Germany, France and the UK have seen particularly high numbers of such requests, with Germany alone witnessing a notable rise. For example, in 2023, Deutsche Telekom reported over 31 000 interception requests, up from around 26 000 in 2022 (https://www.telekom.com/en/company/data-privacy-and-security/news/germany-363566).

80 Sources: Comparitech and Statista.

In that context, communication providers face such challenges in responding to lawful interception requests that they can hardly meet the essential requirements of lawful interception as defined in the Budapest Convention on Cybercrime[81]. Consequently, the operational value of traditional lawful interception is often limited to tactical insights, such as determining whether a device is on or off, the location of the network antenna or who is connected with whom; however, lawful interception of content data transmitted over OTT service providers is most often not possible.

As a result, LEAs are frequently unable to access and read the content of targeted communications[82], or even to understand who is using a given internet service in real time and filter relevant information. This significant loss of access to data in transit affects investigations in several ways:

- major difficulties preventing crimes, mapping criminal organisations and attributing criminal activities committed online or offline;
- increased usage by LEAs of so-called special techniques[83] that are often more intrusive and far more dangerous for officers, for example when the judicial authority prescribes the installation of cameras or microphones close to the target;
- increased usage by LEAs of investigation techniques that are less targeted: without access to communication content or precise geolocation data, investigators often have to investigate **all** persons connected with an individual suspected of criminal activities.

Against that background, the HLG experts flagged four key categories of challenges.

81 https://rm.coe.int/1680081561 [Art. 20 & 21]
82 One expert indicated that content data is not available through traditional LI in 99% of cases.
83 So called special techniques cover a range of tactical means to get information on the target of interest, by means of cameras, microphones, remote access on devices, GPS trackers etc

I. Lawful interception of communications conducted via non-traditional communication providers

Most Member States have implemented some form of regulation governing lawful interception, setting obligations for communication service providers to deploy interception capabilities[84]. While the conditions for issuing lawful interception orders vary significantly between countries, the obligations applying to operators are often similar[85]: they must be capable of intercepting all relevant communications from a specified target on national soil without any gaps, and they must provide the infrastructure necessary to collect and transmit the intercepted data to law enforcement.

In cases where carrier network operators (communication providers who own the network and can access its infrastructure) also provide the communication services (phone calls, SMS, etc.), they are most often able to fulfil lawful interception obligations[86]. In most cases, they build on ETSI standards and rely on specialised technology providers to manage their own constraints including cost-effectiveness, minimal impact on network infrastructure, interoperability, reliability and security.

For OTT services, the situation is more complex: lawful interception can be carried out either by carrier network operators or by the OTT provider delivering the service.

When the interception of communication via OTT services is implemented at carrier network level, its effectiveness is often limited. First, the carrier operator may not be able to identify the target's communications (e.g. when connecting through public Wi-Fi). In addition, OTT services often use proprietary protocols that need to be decoded by lawful interception systems, which adds cost, time and complexity to the process. Finally, the use of end-to-end encryption by OTT providers renders access to content data highly problematic and increasingly prevents access to metadata, as a vast majority of countries consider that carrier network operators' obligation to provide information in clear ends when encryption is implemented by a third party, in line with the Budapest Convention.

---

84 See "Lawful interception – A market access barrier in the European Union", Vadim Doronin in Computer Law & Security Review 51 (2023) 105867

85 Although differences exist on obligations related to content or non-content data.

86 Although features such as home-routing, slicing or Rich Communication Services may hamper the ability of carrier network operators to fulfil their obligations (see section on technological challenges).

The EECC's definition of 'electronic communications services', which has included NI-ICS since 2018, is used by way of reference in Article 5(1) of the ePrivacy Directive. This in turn means that the now-wider concept of ECS (as compared to when the ePrivacy Directive was adopted) makes it possible for Member States to directly rely on OTT providers to perform lawful interception[87]. To date, Member States have made uneven use of this possibility, with some establishing similar obligations for all types of ECS providers, including OTT providers, while others exclude OTT providers[88]. **In practice, regardless of existing obligations, mainstream OTT services have not developed technical mechanisms to respond to lawful interception requests from EU Member States' authorities**, primarily for legal reasons[89].

In contrast, the UK, under the Investigatory Powers Act, has set up a framework for lawful interception of OTT communications which, thanks to the adoption of the UK-US data access agreement, also applies to OTT services based in the US. According to relevant UK authorities, this makes a significant difference in crime prevention and investigations.

Finally, experts from national authorities made clear that tactical interception, based on exploiting vulnerabilities, is neither an effective nor a desirable alternative to enforceable lawful interception rules applicable to OTT providers and should be limited to specific cases, with strong guarantees in place, defined in national laws, to ensure proportionality.

---

87 Although discussions are still ongoing on the exact scope of applicability, and interpretations differ among Member States.

88 See 'Lawful interception – A market access barrier in the European Union', Vadim Doronin in Computer Law & Security Review 51 (2023) 105867.

89 This is not backed up by statistics as national authorities very rarely send LI requests to OTTs, being well aware that doing so is unlikely to yield results.

II. Cross-border requests

Cross-border lawful interception requests directed to OTT service providers and – to a lesser extent – to traditional communication service providers (CSPs) pose several challenges for LEAs.

With regard to traditional CSPs, authorities primarily face organisational challenges. First, international cooperation instruments – notably MLA mechanisms – can be impractical for urgent interceptions requiring authorisation and implementation within hours, not days or weeks[90]. This is due to the number of steps that need to be taken to ensure compliance with the laws in both the requesting and the receiving Member States. The overall perception is that the MLA process is inefficient and burdensome when applied to lawful interception. The European Investigation Order (EIO), which came into application in 2017, replaced the traditional MLA processes within the EU[91], by setting strict deadlines[92] for gathering the evidence requested, limiting the grounds for refusing such requests and introducing a single standard form for authorities to use to request help when seeking evidence. Furthermore, where no technical assistance is needed from the Member State where the subject of the interception is located to carry out the interception, that Member State is notified of the interception through a standard form and given the chance to object to it within 96 hours. In landmark case C-670/22, the CJEU embraced a broad concept of 'interception of telecommunications', holding that the infiltration of terminal devices for the purpose of gathering traffic, location and communication data from an internet-based communication service constituted an 'interception of telecommunications'. The experts nonetheless consider that the significant improvements brought about by the EIO fall short of meeting the need for swift and harmonised cross-border access to data in motion.

In addition, Member States' authorities reported that the existing technical architecture is often not fit for purpose to implement lawful interception in one Member State and transfer the data in near real time to another. In some instances, when relevant organisational protocols are in place, the volume of data to be transferred is simply not compatible with the bandwidth available via secured communication channels.

---

90 Experts mentioned instances where the case was over before the effective implementation of the cross-border LI or cases where the MLA backlog was over 8 months.

91 With the exception of DK and IE, where the EIO does not apply.

92 30 days for the recognition of an EIO and 90 additional days for its execution.

Intercepting OTT communications presents complex jurisdictional issues compared to interception of telephone communications, where providers offer their services in a well-defined territory. Traditional telecom services are tied to a specific physical network infrastructure, ensuring that the service provider has facilities and a legal presence in the country where the interception occurs. This localised setup reduces the risk of intra-EU legal conflicts and makes compliance more straightforward.

In contrast, in the case of OTT services, the requesting authority, the interception target, the physical implementation and the company's place of establishment may span several different jurisdictions. The interplay between legal frameworks in these jurisdictions could potentially result in conflicts of law[93].

Experts from police and judicial authorities are in no doubt: running lawful interception requests through international instruments is not a viable solution. If LEAs bypass the MLA process and instead serve orders directly to service providers under their domestic laws, OTT providers like Microsoft, META or Google may face conflicting legal requirements. For example, in many cases, the requesting Member State would have rules governing lawful access that conflict with Irish law[94], which governs several major OTT providers as they are based in Ireland, but they may also be governed by domestic law in the Member States where they provide their services.

These challenges may be effectively tackled by means of joint measures and some degree of harmonisation of lawful interception rules at EU level in order to facilitate and expedite cross-border requests concerning lawful interception. This would be a prerequisite to address other challenges of an organisational and technical nature, to which solutions can be found when rules are clearly established and workable.

[93] See 'LE interception concerns under the EECC', Microsoft, January 2020.
[94] Irish law prohibits OTT providers from engaging in live interception.

III. Technology

Regardless of legal considerations, the evolution of communication technologies impacts LEAs' technical ability to intercept communications via services provided directly by CSPs or by OTT service providers.

For traditional communication providers, lawful interception capabilities are usually developed by technology providers based on ETSI standards and incorporated in 3GPP[95]. As a result, well-equipped police services can handle the interception of traditional communications – voice and SMS messaging – satisfactorily and can potentially intercept internet-based communications via services provided over their networks.

However, the increasing complexity of communication infrastructures and protocols in 5G, such as virtualisation, network slicing, edge computing and privacy-enhanced features, poses new technological challenges for traditional operators[96]. The HLG experts insisted notably on challenges pertaining to Home Routing[97] and to Rich Communication Services (RCS)[98].

From a forward-looking perspective, and based on the 5G experience, the HLG experts anticipate challenges associated with the future deployment of 6G (foreseen for after 2030) – which will go a step further in terms of privacy-enhancing features[99], possibly involving end-to-end encryption as standard – which, taken all together, could make interception difficult. At the same time, new communication technologies such as IoT, satellite communications and the development of quantum computing[100] are bringing with them another set of challenges to be anticipated.

---

95 Third Generation Partnership Project, which provides the foundation for the development of communication technologies such as 5G, IoT and mobile broadband.

96 See 'Law enforcement and judicial aspects related to 5G', EU Counter-Terrorism coordinator, 2019. https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf.

97 Europol - Position paper on Home routing.pdf (europa.eu).

98 RCS protocol allows the exchange of group chats, video, audio and high-resolution images; it is often used instead of SMS. Depending on its implementation, the lawful interception of RCS messages may be impossible, with significant impact for law enforcement (more than 1 billion RCS active users in 2023).

99 See 6G roadmap: https://smart-networks.europa.eu/wp-content/uploads/2022/12/sns_ri.

100 The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement | Europol (europa.eu).

Finally, the HLG experts highlighted that one of the main technical challenges posed to LEAs comes from end-to-end encryption, notably for OTT communications, with more than 80 % of communications being run through end-to-end encrypted services (live communications and back-up storage), thus preventing investigators from accessing communication content. At the same time, the experts also agree that end-to-end encryption is considered a robust security measure which effectively protects citizens from various forms of crime. By ensuring that only the communicating users can access the content of their messages, end-to-end encryption effectively protects against unlawful eavesdropping, data theft, state-sponsored espionage and other forms of unauthorised access by hackers, cybercriminals, or even the service providers themselves.

Quantifying the challenges that LEAs face in monitoring the communications of criminals and terrorists using end-to-end encryption is difficult. This is because LEAs often choose not to invest the time and resources into obtaining court orders for electronic surveillance on platforms known to use end-to-end encryption by default[101]; hence, the number of effective lawful interception requests for content data that cannot be carried out due to end-to-end encryption is very low and not meaningful. LEAs perceive this lack of surveillance capability as a significant blind spot and vulnerability, one that criminals and terrorists are fully aware of and actively exploit, as demonstrated in the EncroChat[102] and Sky ECC cases which led to thousands of arrests across Europe, including of many high-profile criminals. This concern has been echoed in several statements by the European Police Chiefs[103] and the G7[104], among others. To illustrate the impact of the loss of access to content data, the experts referred to several public examples involving terrorism[105], drug trafficking[106] and rape cases[107], among others, where encryption significantly hampered law enforcement's ability to prevent and fight serious and organised crime.

Law enforcement representatives would prefer an approach that requires companies to provide law enforcement with access to data in clear under strict conditions. It should be noted, however, that cybersecurity experts raised concerns that such solutions would undermine cybersecurity. Some law enforcement experts indicated that in some instances, encryption has been implemented in a way that is compatible with both cybersecurity and the need to maintain some services, such as operating system updates, the scanning of content (e.g. emails or web sessions) for cybersecurity purposes, or key recovery mechanisms when the user opts for this feature.

---

101 Manpearl, 2017.

102 For more on EncroChat and Sky ECC, see Europol and Eurojust, 'Third Report of the Observatory Function on Encryption', June 2021.

103 https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF.

104 https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/g7-london-interior-commitments-accessible-version.

105 In March 2017, Khalid Masood, a 52-year-old man, conducted an Islamist-inspired terror attack in central London, leaving six people dead and 29 injured. While incident reports suggested that Masood had planned and acted alone, it was found that, minutes before he had conducted the attack, he had sent a PDF document entitled 'Jihad' to a large number of his contacts on WhatsApp and iMessage, both of which were – and still are – end-to-end encrypted by default. Sources: Max Hill, 'The Westminster Bridge Terrorist Attack' (London: The Stationery Office, 2018); BBC News, 'WhatsApp Must Not Be a "Place for Terrorists to Hide"', 26 March 2017.

106 Experts mentioned major drug trafficking cases, where no progress was possible until access to encrypted communication through Encrochat and Sky ECC was obtained.

107 In a high-profile case in the UK, police investigations into a rape case were hindered because suspects used WhatsApp to communicate, and the end-to-end encryption made it difficult to access crucial evidence. LEAs' inability to decrypt WhatsApp messages without the user's consent hampered the investigation.

On that basis, law enforcement experts agreed that the challenges posed by encryption demand a multifaceted approach that balances privacy rights, security and the need for law enforcement to be able to access data in order to fight crime and protect people's lives, physical integrity and properties. While a single solution is unlikely to address all of the relevant concerns, a combination of approaches could help mitigate the issue.

IV. Communication providers of a criminal nature

Criminals use mainstream end-to-end encrypted platforms to conceal their communications; however, they can also decide to make use of secure communication channels specifically designed for criminal activity (referred to as 'CCCs', for 'criminal communication channels', in the report)[108]. EncroChat and Sky ECC are both well-known CCCs that sold phones with an integrated end-to-end encrypted messaging service tailored to conceal criminal activities and promoted on the dark web. Both platforms were dismantled in 2020 and 2021 thanks to international joint law enforcement operations that revealed their extensive involvement in organised crime. Several similar platforms, such as Phantom Secure[109] and Exclu[110], have also been dismantled, while many smaller platforms are still operating, providing safe hubs for criminal information exchange. In this fragmented landscape, it is essential that LEAs are able to identify CCCs, monitor and block their activity, dismantle them and bring criminals to justice.

[108] https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf

[109] https://www.fbi.gov/news/stories/phantom-secure-takedown-031618

[110] New strike against encrypted criminal communications with dismantling of Exclu tool | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu)

While operator-based interception is not an option for this type of rogue communication provider, law enforcement needs relevant tactical interception capabilities – tools and expertise – to monitor their users in a targeted manner, despite encryption. Law enforcement experts insisted on the significant challenges, risks and limitations associated with the development and use of such techniques that are not scalable and should be preserved for the most important cases. Depending on their capacities and legal framework, national authorities use different approaches, including tools developed in-house, purchased from third parties or operated as a service; regardless of which option they use, the experts agree that there is a need to have in place guarantees and safeguards for the use of such tools. This may include reflecting on improved oversight, evaluation and certification of the tools, as well as a solid framework on vulnerability management, while fully respecting the procedural autonomy of Member States in criminal matters and their exclusive competence as regards national security.

Investigating authorities are also facing legal challenges, such as difficulties criminalising communication providers and hosting services that offer primarily criminal services (as all traffic is encrypted), which is a necessary first step before taking judicial or administrative action. Moreover, Member States need to be able to impose sanctions on CCCs, with a view to limiting or blocking access to such services in the EU and thus defeating their criminal business model. This will become necessary when and if lawful interception obligations apply to OTT services, so as to prevent criminals from moving back to rogue communication providers.

Finally, different aspects of cases such as those against EncroChat and Sky ECC are challenged in courts. Requirements for using data intercepted in another Member State as evidence vary considerably across the EU, resulting in legal uncertainty for similar operations carried out by one Member State with a potential impact on many.

POSSIBLE SOLUTIONS

I. Make lawful interception requests enforceable for all types of providers of electronic communications services

In the EU, lawful interception capabilities are limited to traditional communication providers, while most communications currently take place via non-traditional communication providers[111]. Whether a communication service is provided by the owner of the infrastructure or not, LEAs' ability to carry out lawful interception on a subject of interest should be the same. Alternative solutions, such as conducting lawful interception on NI-ICS and other communications services exclusively at carrier network level, relying on international cooperation instruments to conduct lawful interception on NI-ICS providers or making extensive use of tactical interception, are not workable[112].

As a result, the HLG experts consider it a priority to ensure that obligations on lawful interception of available data apply in the same way to traditional and non-traditional communication providers and are equally enforceable. The harmonisation of such obligations should serve to overcome the challenges related to the execution of cross-border requests.

To pursue this objective and gradually move towards the approximation and harmonisation of lawful interception rules in the EU, the HLG experts suggest an incremental approach: first, structuring principles should be agreed at EU level (step 1); then, the implementation of those principles should be supported by the Commission (step 2); and finally, based on further assessment, the principles may be codified in a legal instrument (step 3).

---

111 In the UK in 2022, the number of SMS and MMS sent was 36 billion, while the number of online messages was 1.3 trillion (WhatsAppening in the world of online communications? - Ofcom).

112 See section on challenges.

Step 1: Agreeing on a common baseline

First, it is necessary to develop a common understanding of which categories of ECS can be subject to domestic obligations on lawful interception according to ePrivacy and GDPR rules.

Second, it is necessary to reach an agreement on high-level operational requirements that clearly states what is expected by national authorities in terms of lawful interception and what the associated safeguards should be. LEON[113] has been identified as a good basis for defining law enforcement requirements. This document should be accompanied by requirements on e.g. proportionality, oversight and transparency, possibly distinguishing between the rules applicable to content and non-content data, with full respect for cybersecurity and data protection and privacy and without undermining encryption. The possible establishment of an ad-hoc group of experts, including cyber, privacy and law enforcement experts, could ensure that requirements are updated where needed, possibly building on the work of Europol's Working Group on Standardisation on Internal Security, which should be continued.

Third, the concept of territorial jurisdiction needs to be clarified in terms of its applicability to OTT services, taking into account the divergent interpretations among national authorities and, most importantly, between national authorities and OTT providers. For example, the rules applicable to cases where the location of the target is uncertain should be clarified. Guidance is also needed on who can assess the legality of a request, for instance regarding the role of service providers in this context. Last but not least, while the vast majority of court rulings so far have confirmed the legality of procedural acts against EncroChat and Sky ECC, several court cases are still pending[114], with the potential to have a major impact on the conviction of high-profile criminals. Hence, the admissibility of evidence obtained from tactical interception measures between Member States, the mutual recognition of judgments and judicial decisions, and police and judicial cooperation in criminal matters may need to be facilitated.

---

[113] LEON (Law Enforcement – Operational Needs for Lawful Access to Communications) is the outcome of work undertaken by Swedish LEAs, in close cooperation with law enforcement representatives in EU Member States, North America and Australia. The aim is to identify and describe the law enforcement needs for lawful access to communications content, content-related data and subscriber information. See *Communication from the Council Presidency on Law Enforcement Operational Needs for Lawful Access to Communications (LEON)*, 6050/23 of 16 February 2023.

[114] See Cases T-1180/23, T-148/24, T-167/24, T-484/24 and T-560/24.

Recommendation Cluster 7

To agree at EU level on common principles for lawful interception of available data, applicable to all types of providers of ECS, the experts recommend:

1. *clarifying the definition and scope of lawful interception in accordance with existing EU acts and other relevant European and international instruments, such as the Budapest Convention on Cybercrime [recommendation 38];*

2. *taking inspiration from the LEON document to define common operational requirements [recommendation 21];*

3. *identifying necessary safeguards [recommendation 17, recommendation 41];*

4. *addressing the cybersecurity perspective such that no measure should entail an obligation for providers to adjust their ICT systems in a way that would negatively impact the cybersecurity of their users [recommendation 41];*

5. *clarifying the concept of territorial jurisdiction over data to address potential conflicts of law [recommendation 39] and fostering the adoption of minimum rules at EU level allowing for the admissibility of evidence obtained from tactical interception measures between Member States when relevant, to the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters [recommendation 42].*

Consideration needs to be given to the best approach to putting together and agreeing on common principles, as mentioned in Recommendation Cluster 7, and to identifying the most relevant instrument to share those principles. Looking back, the Council Resolution on Lawful Interception from 17 January 1995[115] was instrumental in facilitating the harmonisation of lawful interception solutions as it provided a reference for standards developed by ETSI on lawful interception. A similar approach, possibly through a Commission or Council recommendation, could be equally beneficial.

[115] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104.

Key action: HLG experts call on the EU to issue a Recommendation on real time access to data in 2025

Time: 2025 *Budget: TBD*

- The HLG experts call on the European Commission to issue a Recommendation which clarifies the notion of lawful interception[116] for providers of ECS and details the different requirements that may apply to the lawful interception of available non-content and content data, with full respect for cybersecurity, data protection and privacy, without undermining encryption and building on common operational requirements as defined in the LEON document.

Step 2: Providing EU support to ensure a level playing field and enhance cross-border cooperation

The common principles set out in Step 1 would be the basis for technical, legal and organisational harmonisation at EU level. Their translation into concrete deliverables requires coordination and financial support from the Commission. This would involve setting up a dedicated process, building on existing working groups and, where necessary, creating new ones, ensuring coordination with relevant stakeholders including OTT providers and industry representatives, reporting to relevant bodies, notably the Council and the European Parliament, and ensuring transparency vis-à-vis the public. It could also involve financing targeted studies directly or through relevant partnerships e.g. with relevant agencies or academic partners.

[116] Limited to operator-based interception as defined above.

In addition, the HLG experts stressed the urgent need to improve the efficiency of cross-border lawful interception requests under the current framework, while carrying out the work outlined above. This objective would involve:

- assessing current limitations of the EIO[117] and working on improving operational efficiency;
- addressing technical and organisational limitations pertaining to cross-border exchange of evidence collected through lawful interception, which in turn would require further work on:
    - mapping the problem (what are the limitations, which Member States experience them, etc.),
    - the standardisation of data structures, trust mechanisms and data filtering, to avoid the transmission of non-relevant data and to uphold the data protection principles of purpose limitation, proportionality and data minimisation,
    - the design and capacity of cross-border means of transmissions,
    - identifying associated funding schemes;
- facilitating cross-border lawful interception requests by designating and training SPoCs, in coordination with the broader work on SPoCs and access to digital evidence, with a prominent role for the SIRIUS project;
- where relevant, fostering bilateral agreements between Member States and the US as a prerequisite to facilitate direct requests from national authorities to mainstream OTT service providers, as the scope of the EU-US agreement on cross-border access to electronic evidence currently being negotiated does not, under the negotiating directives, cover lawful interception, which means that specific agreements are needed to address conflicts of law.

[117] The EIO refers to 'telecommunications'; whereas most MS have interpreted it more widely, in line with the EECC update, the possible need to amend the EIO in that regard could be considered and further assessed.

Finally, the experts called for consideration to be given to measures that could improve deterrent measures taken by national authorities against non-cooperative ECS. The experts called, in particular, for the feasibility and proportionality of possible technical solutions to be assessed.

Recommendation Cluster 8

To ensure that a broad range of providers of ECS, including OTT providers, respond to lawful interception requests as set out in national laws, the experts recommend:

1. *supporting the implementation of principles defined in recommendation 1.1 through coordination and funding;*
2. *exploring how the EIO could better support efficient cross-border lawful interception requests e.g. by improving legal certainty, shortening deadlines for responding to orders and fostering a uniform usage of the EIO [recommendation 40];*
3. *building mechanisms (interoperability and cybersecurity) and infrastructures (bandwidth and scalability) that are compatible with the cross-border transfer in real time of large datasets [recommendation 9];*
4. *fostering the designation of SPoCs in the EU to handle requests from and contacts with public authorities, with a view to facilitating the enforcement of obligations on lawful interception and establishing mechanisms for efficient targeting of cross-border requests [recommendations 19 and 36];*
5. *fostering the development of bilateral agreements on real-time access to data with third countries, notably with the United States [recommendation 38.4].*

A number of activities could support the effective implementation of an EU Recommendation on lawful interception.

Key action: HLG experts call for the Commission to accompany the implementation of an EU Recommendation on lawful interception with appropriate coordination and funding

- The HLG Experts call on the Commission to propose a clear plan to support the implementation of an EU Recommendation on lawful interception, including from a financial planning perspective.

Step 3: Assessing the possibility of a legal instrument on lawful interception

Coordination alone may prove insufficient to achieve the level of harmonisation needed, even if complemented by measures to make existing legal instruments more efficient. A new set of rules may be necessary to ensure enforceability of requests and legal certainty, remove conflicts of law and decrease the administrative burden linked to compliance and legality checks. Furthermore, the differences between lawful interception rules across the EU place burdensome requirements upon regulated entities such as OTT providers, potentially creating market access barriers for communication providers[118]. In that respect, harmonised EU rules on lawful interception of available data would help to build Europe's future digital infrastructure, favouring a model where telecommunications infrastructure offers potentially continent-wide coverage[119].

The transition to internet communications is a strong incentive for laying down harmonised access rules at EU level; however, the acceptability, the feasibility and the industry-, cybersecurity- and security-related impact of a legal instrument should be carefully assessed, taking into account the current differences between Member States' legal regimes on lawful interception. The HLG experts stated that a potential instrument should: (i) be in compliance with the principles set out in recommendation 1.1; (ii) fully take into account the fundamental rights perspective and the sovereignty of states in criminal matters and national security; and (iii) take inspiration from the work done on the e-evidence package.

HLG experts agreed that any initiative to foster or impose lawful interception rules on all type of ECS should come with a clear and enforceable framework for taking action against communication providers that operate illegally and/or refuse any form of cooperation with law enforcement. In the absence of such a framework, the rules would be undermined, and criminal actors would, en masse, move their communications to non-compliant providers. Any future EU initiative in this regard should consider the difference between OTT providers that do not fulfil their legal obligations and ECS that deliberately propose services tailored to criminal activities. In addition, any initiative should also factor in the EU *acquis*, in particular the Digital Services Act.

---

118 See 'Lawful interception – A market access barrier in the European Union', Vadim Doronin in Computer Law & Security Review 51 (2023) 105867

119 White Paper - How to master Europe's digital infrastructure needs? | Shaping Europe's digital future (europa.eu)

Such an initiative could encompass administrative or judicial measures. HLG experts called for an in-depth reflection on the matter which would address both fundamental rights and cybersecurity concerns and the complex technological challenges involved.

Recommendation Cluster 9

Based on further analysis and an impact assessment, the experts recommend ***devising an EU instrument on lawful interception (consisting of soft-law or binding legal instruments) for law enforcement purposes*** *that would establish enforceable obligations for providers of ECS in the EU. They recommend that this potential instrument: [Rec 38]*

1. *follow the principles agreed on in Recommendation Cluster 7;*
2. *be technology-neutral [recommendation 21];*
3. *foster the harmonisation at EU level of criminal law measures, including imprisonment, against non-cooperative ECS to enforce cooperation [recommendation 34];*
4. *take into full consideration the fundamental rights perspective and the sovereignty of states in criminal matters and national security [recommendation 38];*
5. *take inspiration from the work done in the context of the adoption of e-evidence rules [recommendation 38, point (iv)];*
6. *place obligations on service providers to turn on or turn off certain functions in their services to obtain information after receiving a warrant (for example, storing the geolocation of a specific user after they are targeted by a lawful request) [recommendation 32];*
7. *include mechanisms to ensure that Member States can enforce sanctions against non-cooperative ECS (either administrative or criminal-law measures, depending on whether a provider is merely non-cooperative or is offering a service of criminal nature), in line with and possibly building on Digital Services Act rules, and that such sanctions act as a deterrent against those entities [recommendation 33].*

Enforcing the principles set out in an EU Recommendation on lawful interception would be an important step towards more harmonised and more enforceable rules on lawful interception. However, a legal instrument may still be needed to improve legal certainty, to ensure that the necessary safeguards are in place for all relevant ECS when implementing lawful interception and to ensure that ECS that are not willing to enforce rules laid down by Member States are compelled to do so.

Key action: HLG experts invite the Commission to assess the further development of the legislative framework on lawful interception for law enforcement purposes

- The HLG experts invite the European Commission to assess, prior to a possible impact assessment, the possibility of an EU legal instrument on lawful interception, building on the work conducted in preparation for the EU e-evidence Regulation and Directive and focusing on identifying potential technology-neutral solutions.

II. Address technological challenges

Many challenges faced by LEAs as regards access to data stem from how difficult it is for them to anticipate technological developments and adapt to them. This is because, in contrast to actors in other sectors such as defence or space, LEAs do not have the resources or the strong relationship with industry needed to do this, and nor are they in the habit of needing to do so. In many cases, internal security actors try to fill technological gaps in a reactive manner or, more commonly, try to cover their needs with off-the-shelf technology that is available and affordable. To foster a shift from a reactive approach to a more proactive one, technological challenges need to be addressed in a structured, forward-looking and multi-disciplinary way, with two main priorities: from the perspective of national authorities, it is essential to ensure that law enforcement has access to the relevant capacities to acquire and process available data in transit; while for operators and technology providers, it is vital that they are able to meet their obligations as regards access to data, privacy and cybersecurity, and that their interests are preserved.

Experts therefore suggest anticipating technological challenges through a comprehensive and forward-looking policy, based on a **technology roadmap for lawful access** that will set objectives and frame activities with associated funding to achieve those objectives.

On capacity building, while the challenges are different, the approach suggested by the experts is often similar for digital forensics, data retention and lawful interception[120] and builds on the same recommendations, with a strong demand for objectives-driven planning to steer funding opportunities, with closer involvement from industrial actors and key stakeholders such as the EU Innovation Hub for Internal Security.

However, law enforcement experts insisted on two elements that are specific to lawful interception.

- Increased use of metadata – e.g. location data, call records and email headers – can provide additional investigative leads. **As more and more devices become connected to the internet, the volume of data generated will increase, offering more opportunities to identify behavioural patterns.** The experts called for more research, innovation and uptake regarding **an extended use of metadata**, for example through AI, as a way to mitigate the lack of access to content data. At the same time, they referred to the risks to privacy associated with extensive AI processing of bulk personal metadata, which need to be balanced with targeted exploitation of content data. However, law enforcement experts are clear that metadata alone cannot fully replace the evidentiary value of communication content for proving intent.

- When criminals are using dedicated end-to-end encrypted communication platforms, LEAs need to make use of tactical solutions based on the exploitation of **vulnerabilities** to gain access to suspects' communications. A number of LEAs already operate under a legal framework allowing for interception at communication endpoints and have the technology to do so, and there is room for further advancements in this regard. This could involve supporting the development of tools made in the EU and allowing LEAs to acquire them and use them under the existing legal framework.

  However, law enforcement experts noted that this method should not be expanded as a primary means of evidence collection as tactical interception is neither scalable nor without problems. For instance, jurisdictional issues could arise based on the target's location. Moreover, the use of vulnerabilities that cannot be disclosed inevitably contradicts core cybersecurity principles.

[120] Detailed in the chapter on digital forensics.

On lawful access by design, law enforcement experts suggested a cautious approach, as industry actors should not be asked to integrate any system likely to weaken encryption in a generalised or systemic way for all users of a service; lawful access should remain targeted, on a communication-by-communication basis. They agreed on the relevance of the overall objective, but they insisted on the need to advance gradually and to involve all relevant categories of stakeholders, including technology, cybersecurity and privacy experts, taking into account the potential risks and the sensitivity of public debate. In particular, they strongly advised taking an evidence-based approach and carefully assessing the availability of technical solutions that do not weaken the cybersecurity of communications or negatively impact the cybersecurity of operators.

Recommendation Cluster 10

To address the technological challenges of lawful interception, the experts recommend developing ***a technology roadmap for lawful access***[121] *that will in particular:*

1. *bring together technology, cybersecurity, privacy, standardisation and security experts and ensure adequate coordination, potentially through a permanent structure [recommendation 22];*
2. *foster research into and development and uptake of tools for data acquisition and access to data, including decryption capabilities, as well as AI-based capacities for data analysis*[122] *[recommendation 4];*
3. *foster a coordinated approach to standardisation that would take into consideration, as appropriate, the needs for lawful access to data and would also [recommendations 15, 16 and 20]:*
    a. *foster the involvement of practitioners from all relevant communities in relevant standardisation groups;*
    b. *accompany future initiatives with adequate standardisation measures (to foster a technology-neutral approach);*
    c. *cover communication technologies at large, IoT (including, for example, connected cars) and any form of connectivity (including, for example, satellite communication);*
4. *enhance EU coordination with industry to address situations where technological solutions exist but are not implemented; in such cases*[123]*, clear guidance and dialogue facilitated at EU level is necessary [recommendation 24];*
5. *implement lawful access by design with regard to all relevant technologies in line with the needs expressed by law enforcement, ensuring at the same time strong security and cybersecurity and that legal obligations on lawful access are met [recommendation 22];*
6. *address, in a thorough manner, the challenges of encryption by:*
    a. *ensuring that possible new obligations and/or standards do not lead, directly or indirectly, to obligations for the providers to weaken communication security by generally undermining or weakening end-to-end encryption [recommendation 23];*
    b. *ensuring that lawful access by design does not have a negative impact on the security posture of the hardware or software architectures involved [recommendation 23];*
    c. *working in a coordinated manner and with the support of EU funding on a methodology to develop, handle and use targeted lawful access to address cases where access to data is not possible through cooperation with ECS [recommendation 10].*

---

121 The technology roadmap should cover the three workstreams: digital forensics, data retention and lawful interception.

122 This recommendation also applies to accessing data on a device (see section on digital forensics), but the use cases are slightly different.

123 For example, when home-routing agreements or a specific kind of implementation of RCS do not allow for lawful interception.

While some initiatives suggested by the HLG experts already partially exist, there is a strong need to better structure the technological mid-term and long-term policy on lawful access in the technology roadmap, with targeted objectives and an associated monitoring instrument. This approach should not only cover access to data in transit, but also digital forensics and data retention.

The technology roadmap should be forward-looking, enforceable, focused on priority topics and anchored in the EU's digital strategy. It should involve all relevant categories of stakeholders, in particular EU institutions, bodies and agencies, national authorities, academics across all relevant fields, industry and NGOs, in close partnership, and have clear governance.

Key action: HLG experts urge the Commission to put forward and implement a technology roadmap on access to data

- The HLG experts call on the European Commission to draw up and implement a technology roadmap focusing on encryption challenges, addressing all relevant aspects, including technological, market, cybersecurity, fundamental rights, standardisation, law enforcement and research aspects. This technology roadmap should be available in 2025 and should build on all relevant expertise from Member States and EU institutions bodies and agencies, including on cybersecurity, data protection and privacy.